

**Department of Veterans Affairs  
Veterans Health Administration (VHA)**



**Michael E. DeBakey  
VA Medical Center**

**Privacy Policy and Procedures**

**Revised May 2020**

**1. PURPOSE..... 3**

**2. POLICY..... 3**

**3. RESPONSIBILITY ..... 4**

**4. PROCEDURES ..... 15**

**A. Administrative Requirements..... 15**

    I. Compliance with Privacy Policies..... 15

    II. Documentation..... 15

    III. Complaint Process..... 16

    IV. Reasonable Safeguards..... 20

    V. Sanctions ..... 25

    VI. Privacy Training and Education..... 26

    VII. Privacy Threshold Analysis..... 28

    VIII. Privacy Impact Assessment ..... 29

    IX. Personally Identifiable-Information Database Inventory ..... 30

**B. Individual Rights..... 30**

    I. Verification of Identity..... 30

    II. Right of Access ..... 32

    III. Notice of Privacy Practices ..... 33

    IV. Amendment Request ..... 34

    V. Confidential Communications Request ..... 38

    VI. Restriction Request..... 40

    VII. Facility Directory Opt-Out ..... 42

    VIII. Accounting of Disclosures ..... 43

**C. Uses and Disclosures ..... 45**

    I. Minimum Necessary..... 45

    II. Authorizations ..... 46

    III. Processing a Request for Release of Information ..... 51

    IV. Uses/Disclosures for Treatment, Payment, and Health Care Operations, and Other Operations Not Requiring Authorization ..... 53

    V. Deceased Individuals ..... 61

    VI. Contracts and Business Associate Agreements ..... 62

    VII. Emergency Situations and Serious and Imminent Threats ..... 63

    VIII. Standing Written Request Letters ..... 65

    IX. State Prescription Drug Monitoring Program..... 67

    X. De-identification of PHI ..... 67

    XI. Research Activities: General..... 68

    XII. Research Activities: Use..... 69

    XIII. Research Activities: Disclosure ..... 70

    XIV. Logbooks ..... 74

**D. Freedom of Information Act (FOIA)..... 74**

    I. General ..... 74

    II. Requests for Copies of Records ..... 76

    III. Processing a FOIA Request..... 77

IV. Coordination with District Counsel and VHA FOIA Officer ..... 80  
V. Annual Report of Compliance with FOIA..... 80

**APPENDIX I: Glossary of Terms..... 81**

**APPENDIX II: Acronyms..... 88**

VHA PRIVACY POLICY AND PROCEDURES

**MICHAEL E. DEBAKEY VAMC**  
Houston, Texas 77030

**Rescinded Document:**  
00APO-001 Privacy  
Policy and Procedures,  
August 4, 2017

**Signatory Authority:**  
MEDVAMC Director

**Effective Date:**  
June 1, 2020

**Responsible Owner:**  
Privacy Officer

**Recertification Date:**  
June 1, 2025

1. **PURPOSE**

- A. This memorandum implements facility privacy policy in compliance with Veterans Health Administration (VHA) Directive 1605.01, Privacy and Release of Information, and establishes responsibilities and procedures for the privacy protection of information that is accessed, collected, maintained, used, disclosed, transmitted, amended and/or disposed of by the staff and systems of this facility.
- B. The components in this policy are designed to meet all of the specific requirements of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and VA/VHA policy. If any of the policy elements contained herein is removed, this facility policy will not be fully compliant.
- C. In this document, the term workforce refers to on-site or remotely located employees, residents, students, Without Compensation (WOC) staff, volunteers, and any other appointed workforce members. Contractors will be held responsible for adhering to these policies and procedures in accordance with contracts and Business Associate Agreements (BAA).

2. **POLICY**

- A. This facility will develop, implement, maintain, and enforce a structured privacy program to properly use, disclose and safeguard individually identifiable information. The privacy program is designed to allow continued operation of mission-critical activities while ensuring the

integrity, availability, confidentiality, and authenticity of data and information; minimum necessary access to protected health information; and a continuing awareness of the need for, and the importance of, information privacy within the facility.

- B. All members of the workforce are responsible for complying with this privacy policy, applicable federal laws and regulations, VA/VHA policies, as well as the procedures and practices developed in support of these policies. All facility privacy policies and procedures must be consistent with VHA 1605 Directives and Handbooks.

All privacy and other workforce members responsible for implementing and complying with these policies and procedures will be provided copies of, or access to, this policy. Violations of privacy policies or procedures will be brought to the attention of management for appropriate disciplinary action and/or sanctions, and reported in accordance with national and local policy. Privacy violations will be reported through the Privacy and Security Event Tracking System (PSETS) to the VA Cyber Security Operations Center (VA-CSOC) by the facility Privacy Officer within one hour of the time it is discovered by the Privacy Officer. In the absence of the Privacy Officer, staff are required to report violations to an alternate or delegate who will then be responsible for reporting the incident within one hour of their discovery. The Information Systems Security Officer (ISSO) or Alternate Privacy Officer may also open PSETS in the absence of the Privacy Officer. Outside of normal business hours incidents will be reported to the MEDVA MC police service.

- C. All policies and procedures, and any actions/activities taken as a result of a privacy complaint/violation, must be documented in writing and a written response letter must be given or sent to the complainant. In addition to policies and procedures, privacy-related communications, decisions, actions, and activities or designations, including any signed authorizations, must be documented and kept in a complaint file. All documentation must be retained in accordance with the VA records control schedule (RCS-10).
- D. All documentation related to the information privacy program will be reviewed and updated as needed in response to operational changes affecting the privacy of individually- identifiable information (III).
- E. Medical Center Director is responsible for designating a facility Privacy Officer and a FOIA Officer in writing. The facility must identify at least one alternate Privacy Officer and FOIA Officer to allow for coverage when the designated Privacy and FOIA Officer is unavailable.

### 3. **RESPONSIBILITY**

- A. **Executive Management (Director, Associate Director, Chief Nursing Executive, Chief of Staff)** is responsible for:
- I. Providing the necessary resources (funding and personnel) to support the Privacy Program, maintaining a culture of privacy, and ensuring that the facility meets all the privacy requirements mandated by VA/VHA policy and other federal legislation [e.g., Freedom of Information Act (FOIA) [5 U.S.C. § 552], Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule [45 C.F.R. Parts 160 and 164], Health Information Technology for Economic and Clinical Health (HITECH) Act, Privacy Act (PA) [5 U.S.C. §552a], VA Claims Confidentiality Statute [38 U.S.C. 5701], Confidentiality of Medical Quality Assurance Review Records [38 U.S.C. 5705], and Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Medical Records [38 U.S.C. §7332]].
  - II. Ensuring Privacy Officer coverage for the facility and its associated clinics. It is required by VHA Privacy Policy that the facility Privacy Officer report directly to the Medical Center Director, Associate Director. When the facility Privacy Officer or Alternate is not available, provide coverage for off-hours operations if conducting 24/7 operations.
  - III. Ensuring facility Privacy Officers are fully involved in all projects concerning the access, collection, maintenance, use and/or disclosure, transmission, amendment, and/or disposal of III.
  - IV. Ensuring that new and revised Memorandums of Understanding (MOU), Contracts, Data Use Agreements (DUA), Business Associate Agreements (BAA), or similar agreements which involve the collection, transmission, use or sharing of information are reviewed by the facility Privacy Officer, in accordance with VA Handbook 6500.6, Contract Security, prior to approval by Executive Leadership.
  - V. Ensuring that the facility Privacy Officer is included in discussions and privacy concerns of the facility, which are addressed in strategic initiatives, and maintains a facility culture of privacy.
  - VI. Cooperating with the facility Privacy Officer in any investigation, mediation strategies, or correspondence that is required in order to investigate and resolve a complaint or

allegation and ensuring that appropriate disciplinary action is taken.

- VII. Certifying annually or on an as needed basis, to the VHA Privacy Office, that privacy training has been completed for all personnel. This shall include all employees, volunteers, contractors, students, residents, and any other person performing or conducting services on behalf of the facility.
- VIII. Cooperating fully in submissions of Facility Self-Assessments (FSA) and ensuring full facility wide cooperation for Privacy Compliance Assurance Assessments both on-site and remote as required by the Privacy Compliance Assurance (PCA) Office.
- IX. Ensuring that signs are placed alerting Veterans to auditory privacy concerns in areas, elevators, and other spaces requiring auditory privacy and ensuring that facility employees exercise appropriate precautions and safeguards when discussing Veterans' individually identifiable information in public areas, such as clinic waiting rooms.

**B. Privacy Officer** is responsible for:

- I. Developing, implementing and updating local privacy policies and procedures.
- II. Reviewing all health care center policies to ensure compliance with all privacy laws and regulations
- III. Conducting periodic assessments, compliance reviews and/or audits of the facility's collection, use, storage and maintenance of personal information. Assessments will include identification and correction of privacy vulnerabilities related to incidental disclosure such as posted and displayed PHI in clinical areas.
- IV. Establishing effective working relationships with the facility Information System Security Officer (ISSO), Area Manager Contracting Officer, < Research Compliance Officer, if applicable>, Compliance Officer, and Human Resources Management personnel to ensure that local policies and procedures which may impact the privacy program support and complement each other.
- V. Ensuring that Executive Leadership is apprised of all privacy vulnerabilities and related issues.

- VI. Coordinating with the facility Information System Security Officer (ISSO) for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule, HITECH or other federal privacy statutes.
- VII. Serving as the facility's point of contact (POC) for matters relating to the privacy policies and procedures.
- VIII. Ensuring that members of the workforce receive training and education about privacy policies and procedures as required by VHA Privacy Program.
- IX. Ensuring that members of the workforce know whom to contact when a privacy complaint or incident is identified or received.
- X. Monitoring facility and workforce compliance with VHA privacy policies and procedures as well as compliance with local privacy policies and procedures.
- XI. Identifying and reviewing areas within the facility for auditory privacy risks, to ensure appropriate safeguards are in place to limit incidental disclosures. Ensure the placement of signs alerting Veterans and staff to auditory privacy concerns in the waiting areas, elevators, and other spaces requiring auditory privacy and ensure the placement of chairs in waiting areas are optimally placed to minimize auditory privacy violations.
- XII. Ensuring the placement of signs prohibiting the use of camera phone or video in restricted areas are in compliance with VHA Directive 1078.
- XIII. Ensuring processes are in place for the appropriate accounting of disclosures of individually identifiable information made by the facility and appropriate utilization of the ROI Plus software or other tracking mechanism are used in accordance with the facility's policies and procedures. The processes will include accounting for authorizations electronically conducted through iMed Consent.
- XIV. Collaborating with various program officials and the Contracting Officer, to ensure identification of all entities meeting the definition of Business Associates.



- XV. Maintaining a list of active Business Associates utilized by the facility and ensuring all Business Associates have a signed BAA in place prior to disclosure of individually identifiable health information (IIHI) and that the Business Associate adheres to the requirements of the BAA.
- XVI. Collaborating with the Records Manager to ensure that RCS 10-1 is followed for record control requirements and no unauthorized system of records are being kept. The Privacy Officer queries the Record Manager on an annual basis to ensure facility file plans are updated and records are maintained securely, archived properly, destroyed properly, and monitors are completed in compliance with VHA Directive 1605.03
- XVII. Ensuring all facility developed paper, web-based or electronic forms that collect personal information contain the appropriate Privacy Act statements. The Medical Records Committee (MRC) will review all forms, which are contained in a Privacy Act System of Records to ensure the Privacy Act statements are included on all forms.
- XVIII. Reviewing and approving all MOUs, Contracts and/or DUAs when required for the sharing of VA sensitive data between the facility and other parties.
- XIX. Ensuring prompt investigation and follow-up on allegations or known occurrences of privacy violations or complaints including logging the violation or complaint in the Privacy and Security Event Tracking System (PSETS). PSETS should be initiated upon notification of the violation during normal business hours, within one hour of discovery during normal business hours or as soon as possible outside of normal business hours. If a privacy violation presents the risk of media involvement, congressional inquiry, legal action , immediate harm to any individual or any other high-risk outcome, the incident must be reported within one hour of discovery regardless of discovery time (even during non-business hours).
- XX. Reports promptly to the VHA Privacy Office any potential privacy complaint, allegation, or activity that has VISN-level or national-level impact.

- XXI. As a non-voting member of the facility Institutional Review Board , the Privacy Officer will review all human subject research protocols, exempt and non-exempt, in accordance with VHA Handbook 1200.05 and other applicable guidance to ensure legal authority exists prior to use and disclosure of VHA information for research.
- XXII. Collaborating with the facility Information System Security Officer (ISSO), Area Manager and System Owner to ensure that a Privacy Threshold Analysis (PTA) and a Privacy Impact Assessment (PIA) if applicable is completed on all information technology systems, applications or programs that collect, maintain, and/or disseminate personally identifiable information (PII).
- XXIII. Reviewing, processing, and monitoring requests to amend any information or record retrieved by an individual's name that is contained in a VA system of records, to include designated record sets, and coordinating such amendments with the author of the document.
- XXIV. Collaborating with the facility Information System Security Officer (ISSO), Contracting Officer Representative (COR) and the Contracting Officer to ensure all contracts are reviewed in compliance with VA Handbook 6500.6.
- XXV. Ensuring all facility's policies and procedures relating to HIPAA, HITECH, Privacy Act, 38 U.S.C. §5701, §5705, and §7332, and FOIA are consistent with current guidelines and requirements, complementing and supporting each other.
- XXVI. Ensuring local departmental policies and procedures are developed if not specifically outlined in the facility Privacy and FOIA policies.
- XXVII. Provide awareness training through various means for Veterans to inform them of their privacy rights and responsibilities.
- XXVIII. Complete the Facility Self-Assessment by the last business day of each quarter or as required by PCA and work with facility staff and leadership to facilitate a successful on site and remote Privacy Compliance Assessments.
- XXIX. Ensuring that the reduction of SSN usage is reviewed to determine the necessity.

XXX. Other responsibilities as defined by the VHA Privacy Office.

C. **FOIA Officer** is responsible for:

- I. Ensuring that all FOIA requests for Federal records that would not otherwise be disclosed in accordance with HIPAA or the Privacy Act, e.g. Withholding of information in accordance with 38 USC 7332 are processed.
- II. Ensuring that all FOIA requests or HIPAA/PA requests where information was withheld under a FOIA exemption are entered into FOIAXpress within required time frames.
- III. Notifying the VHA FOIA Office upon receipt of a Substantial Interest request on the same date of receipt.
- IV. Other responsibilities as defined by the VHA FOIA Office.

D. **Information System Security Officer (ISSO)** is responsible for:

- I. Coordinating with the facility Privacy Officer for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule, HITECH or other federal privacy statutes.
- II. Coordinating, facilitating, and updating the establishment of information security policies and procedures, to work in tandem with privacy policies and procedures.
- III. Establishing effective working relationships with the facility Privacy Officer, Area Manager, Contracting Officer, Research Compliance Officer, Compliance Officer, and Human Resources Management personnel to ensure that information technology (IT) security and HIPAA/FOIA/PA/Federal Information Security Management Act (FISMA) policies and procedures compliment and support each other.
- IV. Reviewing and evaluating the security program impact(s) of any proposed facility information privacy policy and procedure changes.
- V. Collaborating with the facility Privacy Officer on addressing/resolving privacy complaints, investigations, and access rights to audits and other information maintained by the facility Information System Security Officer (ISSO).

- VI. Collaborating with the facility Privacy Officer, Area Manager and System Owner to ensure that the Privacy Threshold Analysis (PTA) and the Privacy Impact Assessment (PIA) if applicable is completed and fully executed on all information technology systems, applications or programs that collect, maintain and/or disseminate personally identifiable information (PII).
  - VII. Entering all Information Security violations through the Privacy and Security Event Tracking System (PSETS) to the VA Cyber Security Operations Center (VA-CSOC) within 1 hour of discovery
- E. **Clinical staff or designees** are responsible for:
- I. Reviewing and determining appropriateness for granting individuals' requests for record amendment.
  - II. Accessing, using and disclosing protected health information only when legal authority exists.
- F. **Area Manager** or designee is responsible for:
- I. Coordinating with facility Information System Security Officer (ISSO) and facility Privacy Officer to provide technical advice and other assistance relative to the reasonable safeguards requirements of privacy statutes and regulations dealing with implementation of IT systems, policies and procedures.
  - II. Identifying each locally maintained computer system that contains III and providing technical input for various mandated documents, reports, and investigations.
  - III. Ensuring all computer rooms meet acceptable reasonable safeguards and that minimum necessary access is maintained.
  - IV. Collaborating with the ISSO, Privacy Officer and System Owner to ensure that the Privacy Threshold Analysis (PTA) and the Privacy Impact Assessment (PIA) if applicable is completed and fully executed on all information technology systems, applications or programs that collect, maintain and/or disseminate personally identifiable information (PII).
- G. **Chief, Human Resources Management Service (HRMS)**, or designees are responsible for:

- I. Providing consistent and uniform guidance to supervisors and managers regarding personnel actions, sanctions, or other actions to be taken when employees have violated information privacy practices, laws, regulations, policies and procedures, and rules of behavior (see VA Directive 5021).
  - II. Ensuring that appropriate disciplinary action is taken.
  - III. Providing appropriate information to facility Privacy Officer for completion of PSETS entries in a timely manner regarding mitigation/disciplinary actions.
  - IV. Coordinating with facility Privacy Officer on the privacy and disclosure of personnel records and other records maintained by HRMS.
  - V. Ensuring that personnel records maintained by the HRMS are maintained in compliance with applicable privacy policies, statutes and regulations.
- H. **VA Contracting Officer/Contracting Officer Representative (COR)** is responsible for:
- I. Determining the appropriate security and privacy language in all contracts by collaborating with the facility Privacy Officer to ensure that privacy responsibilities are included (see VA Directive 6500.6, Appendix C).
  - II. Ensuring through the COR that contractors are aware of, and abide by, those privacy responsibilities as stated in contracts with VA and VHA.
  - III. Ensuring that Business Associate Agreements are enacted for contracts which the contractor meets the definition of a Business Associate. A BAA should be a separate document from the contract.
  - IV. Ensuring that contractors receive the appropriate privacy and, if applicable, security training upon initiation of the contract and annually thereafter.
  - V. Ensuring that contract performance meets privacy requirements including mediating and/or terminating the contract if information privacy requirements are not being met.

- I. **Local Managers, Supervisors**, and their designees are responsible for:
  - I. Identifying and protecting all individually identifiable information (III) used by supervised personnel, including contractors and other workforce members. Ensuring that individuals are only provided access to III when authorized and the appropriate training has been completed such as in the case of volunteers. (Note: CWT, compensated work therapy patients are prohibited to have access to PHI).
  - II. Ensuring that III, whether computerized or printed, is secured when work areas under their supervision are unattended.
  - III. Facilitate or provide training to new and existing personnel on roles and responsibilities for protecting III, to include the requirement that possible suspected privacy violations are reported to the Privacy Officer at the time of discovery.
  - IV. Identifying functional categories in accordance with facility policy and ensuring VA personnel have only the minimum necessary access level required to carry out their authorized functions or assigned duties and that VA personnel understand what their minimal level of access is and that access beyond the scope of their responsibilities will result in disciplinary action.
  - V. Ensuring applicable personnel complete the “Information Security and Privacy Awareness and Rules of Behavior” training. If access to protected health information (PHI) is required then “Privacy and HIPAA Focused” training must be completed within 30 days of hire or before access to PHI is given. Training must be completed annually thereafter and documented using the Talent Management System (TMS). Workforce members must be enrolled in TMS through either self-enrollment (e.g. contractors and volunteers) or automatic enrollment upon hire.
  - VI. Ensuring that all media (paper, electronic, CDs, disks, portable devices, etc.) with III is disposed of via approved means. This is accomplished by taking the electronic media to the OI&T Help Desk for disposal. Media with III will be shredded or placed in a locked recycling receptacles for final disposition. All discarded paper documents containing III/PHI must be disposed of by placing into the locked shred bin provided by Facilities Management.

- VII. Assists the facility Privacy Officer and Human Resource Management Service with the investigation and resolution of privacy incidents involving their employees and/or program(s), however, supervisors are not to access a record for investigation without express permission from the Privacy Officer.
- VIII. Provide all responsive documents to the FOIA Officer upon request in a timely manner and require cooperation from staff in response to all FOIA requests.
- J. Quality Manager serves as Quality Management (QM) Confidentiality Officer and is responsible for coordinating with the facility Privacy Officer on requests for copies of or access to QM documents. The facility Privacy Officer serves as the final approval authority for determining which documents are classified as quality management documents in accordance with VHA Directive 2008-077, Quality Management (QM) and Patient Safety Activities That Can Generate Confidential Documents prior to disclosure. The facility Privacy Officer will work with the FOIA Officer concerning any exception to disclosure under FOIA.
- K. Administrative Officer of the Day (AOD) is responsible for resolving and responding to disclosure issues and incident reporting requirements consistent with VHA Directive and VHA Handbooks 1605 series, VA Directive 6500 and VA Handbook 6500 series during non-business hours. The AOD is also responsible for providing copies of health records to non-VA provider/hospital when urgent. Otherwise, the AOD will provide non-VA provider request to the ROI Unit for processing.
- L. All Employees
  - I. Accessing the minimum necessary data for which they are authorized in accordance with all laws and regulations in the performance of their official VA duties.
  - II. Employees must exercise appropriate precautions and safeguards when discussing Veterans' individually-identifiable information in public areas to prevent an unauthorized disclosure.
  - III. Protecting an individual's rights to privacy and ensuring proper use and disclosure of information. All workforce members will be held accountable for compliance with these policies, procedures, and applicable laws.

- IV. Appropriately safeguarding printed and electronic individually identifiable information.
- V. Reporting complaints and/or violations of privacy policies or procedures to the facility Privacy Officer immediately upon discovery.
- VI. Obtaining appropriate approval in accordance with Public Affairs policy to speak to the news media. Employees are not authorized to disclose any individually-identifiable information on a patient or Veteran during an interview without the prior signed, written authorization of the patient or Veteran. When an employee is asked to be interviewed by a third party, such as the news media, VA Form 10-3203a, Informed Consent and Authorization for Third Parties to Produce or Record Statements, Photographs, Digital Images, or Video or Audio Recordings must be completed.
- VII. Consulting the facility Privacy Officer and VHA Directive 1605.01 for guidance in privacy situations not addressed in this document.

#### **4. PROCEDURES**

##### **A. Administrative Requirements**

- I. Compliance with Privacy Policies
  - a. The facility and its workforce will comply with the contents of this policy, VHA Directive 1605.01, and all other applicable privacy laws, regulations, and VA policies.
  - b. The facility Privacy Officer will monitor compliance with this policy through various means, including continuous assessment for privacy compliance.
- II. Documentation
  - a. This policy and any changes thereto, must be maintained in writing, either on paper or in electronic form, for a period of at least six (6) years.
  - b. Changes in VHA Directive 1605.01: When VHA Directive 1605.01, is updated which necessitates alteration of facility policies and procedures, the local



privacy policies and procedures will be revised without delay. See local policy 00Q-020 Medical Center Publications.

### III. Complaint Process

- a. All privacy complaints received by the facility are to be referred immediately to the facility Privacy Officer or Alternate Privacy Officer for review and processing.
- b. An individual has 3 years from the date of the complaint to request an investigation into the alleged complaint. Health and Human Services, Office for Civil Rights uses this same time frame for their complaints.
- c. The facility Privacy Officer, Alternate or ISSO will enter all facility privacy incidents and complaints, regardless of validity, into the VA Privacy and Security Event Tracking System (PSETS). Employees can report privacy incidents during business hours to the Privacy Officer/Alternate or Information System Security Officer by securely emailing [vhahouprivacyoffice@va.gov](mailto:vhahouprivacyoffice@va.gov) or [vhahouiso@va.gov](mailto:vhahouiso@va.gov). After hours incidents should be reported to the VA Police Department. All incidents must be reported within one hour of discovery to the VA Cyber Security Operations Center (CSOC).
- d. Notice to Privacy Complainants: All individuals filing a privacy complaint, i.e., privacy complainants, will be provided a copy of the Notice to Privacy Complainants at the time of the complaint submission regardless of the way it was received (e.g. email, mail or verbal).
  - 1) If the complaint is made verbally, the Privacy Officer, or Alternate Privacy Officer will obtain mailing information in order to send the Notice to Privacy Complainants.
  - 2) The Notice to Privacy Complainants will be mailed to the privacy complainant within 2 business days if the Notice is not given in person to the complainant. A complaint acknowledgement cover letter will be included when the Notice is mailed.
- e. The facility Privacy Officer is responsible for:

- 1) Investigating all complaints regarding facility privacy practices regardless of validity.
- 2) All employees are required to fully cooperate with the facility Privacy Officer and/or the VHA Privacy Office throughout the complaint investigation process.
- 3) Cooperating with the VHA Privacy Office on all HHS-OCR complaints and all other privacy complaints submitted to VHACO, in addition to providing timely access to complaint investigation files.
- 4) Acknowledging receipt of the privacy complaint in writing.
- 5) Communicating with leadership, as appropriate (i.e., Director, VISN, VHA Privacy Office, Office of Inspector General, and Office of General Counsel).
- 6) Determining the validity of a complaint or incident and responding appropriately.
- 7) Responding as soon as possible or no later than 60 calendar days, in writing to the complainant when the complaint does not result in an incident.
- 8) Appropriately notating the privacy complaint/incident in PSETS.
- 9) Documenting outcomes of the investigation and provide findings to the supervisor in coordination with other stakeholders (i.e., Human Resources for sanctions or disciplinary actions, union representatives, department heads).
- 10) Maintaining an administrative file for all complaints by PSETS ticket number or by date.
- 11) Trending the types of privacy complaints identified and reports these trends to the facility leadership bi-annually and VHA Privacy Office, upon request.

- f. **Complaints Identified as Incidents:** When the facility Privacy Officer makes a determination during the investigation that a privacy complaint is a privacy incident, the PSETS ticket classification will promptly be changed from a complaint to an incident.
- 1) When a privacy complaint is made regarding access to a health record and the facility Privacy Officer cannot determine that the access is likely or not likely authorized, the access must be presumed to be unauthorized and will be reported as a privacy incident in PSETS.
  - 2) All determinations as to whether or not a privacy incident warrants credit monitoring protection services or a notification only letter will be made by the VA Data Breach Resolution Service (DBRS) and the Data Breach Core Team (DBCT).
  - 3) The DBRS and DBCT will notify the facility Privacy Officer in accordance with VA Directive 6500.2, Appendix C.
  - 4) When required the HIPAA notification letter or credit monitoring letter will be mailed no later than 60 calendar days from when the incident was reported by the facility Privacy Officer.
- NOTE:** The date reported is considered the date the Privacy and Security Event Tracking System (PSETS) ticket was entered by the Privacy Officer.
- g. **Administrative Record Keeping:** A privacy complaint file containing all of the documentation of the privacy complaint and investigation will be retained by the facility Privacy Officer in accordance with Record Control Schedule (RCS) 10-1, XL III-8, and Privacy Complaint File. Documentation will consist of the following:
- 1) Initial written complainant's concern or a Report of Contact by the facility Privacy Officer, if the complaint is made orally;
  - 2) Written documentation of all interviews or statements; and

- 3) All written correspondence, including e-mails.
- h. All complaints (privacy and/or security related) received by the facility from the Department of Health and Human Services (HHS)-Office for Civil Rights (OCR) will be forwarded immediately to the VHA Privacy Office in VHACO for appropriate processing. The facility does not have authority to respond to HHS-OCR complaints. However the expectation is that the PO will repond timely to any questions that the VHA privacy office needs in order to respond to HHS OCR.
- 1) If an investigation arises as a result of a HHS-OCR complaint, this facility and its Business Associates must permit the Secretary of HHS access to information, during normal business hours, after coordinating with the VHA Privacy Office.
  - 2) If the facility Privacy Officer receives a HHS-OCR notification letter, this notification letter should be forwarded via encrypted e-mail to the:  
[VHAPrivacyIssues@va.gov](mailto:VHAPrivacyIssues@va.gov) outlook mail group.
- i. When addressing complaints the facility Privacy Officer should reference resources available on the VHA Privacy Officer Share point site.  
<https://vaww.vets.vaco.portal.va.gov/sites/privacy/vhapo/Pages/ComplaintTracking.aspx> When Human Resources is contemplating employee disciplinary action, they should refer to VA Directive 5021 and VA Handbook 5021, Employee/Management Relations.
- j. The facility may not retaliate against a person for exercising rights provided by the HIPAA Privacy Rule, for assisting in an investigation by HHS-OCR or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates these provisions.
- k. The facility may not require an individual to waive any right under these provisions as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

## IV. Reasonable Safeguards

- a. All facility workforce members shall ensure that appropriate administrative, technical, and physical safeguards are used to maintain the security and confidentiality of III, including protected health information (PHI), and to protect against any anticipated threats or hazards to their security or integrity. The facility's personnel shall make reasonable efforts to limit III to the minimum necessary to accomplish the intended purpose of any use, disclosure, or request. This does not pertain to the treatment provision under the HIPAA Privacy Rule.
- b. All personnel may access and use information contained in VHA records as required for their official duties related to treatment, payment, and health care operations purposes.
- c. When disclosing VHA information, all applicable laws and regulations are reviewed and applied to the request in order to assure utilization of the most stringent provisions for all uses and/or disclosures of data in order to provide the greatest rights to the individual and the minimum necessary of III. III disclosure is mandatory with a valid written authorization, signed by the individual but disclosure must be limited to only the information necessary to satisfy the purpose of the request.
- d. Disposal of Paper Documents: Staff disposes of paper documents that contain III by utilizing the locked recycling bins provided by Facilities Management throughout the hospital and other buildings. These bins are emptied and shredded on site per VHA requirements by a local contractor who will then take the shredded material to be pulverized. Only VA approved shredders can be utilized by VA staff rather than using the recycling bins when shredding VA sensitive information.
- e. Disposal of Electronic Media: Electronic media containing III will be destroyed by degaussing and reused, or rendered useless by shredding, hole punching or burning. Defective or damaged magneticf

storage media that have been used in a sensitive environment shall not be returned to the vendor (will be annotated in all contracts/ SOW's) This is required since many ERASE commands do not actually erase the file. The Area Manager, ISSO, Biomed or designee's will be responsible for this process. Other media that is not destroyed at the site of production, such as that which is transported for contracted shredding must be secured in locked containers or in locked areas until it is removed for destruction. OIT may be contacted for assistance.

- f. Disposal of Non-paper Items: Non-paper items (i.e. I.V. bags, wristbands, prescription bottles, etc.) containing III are destroyed by staff who will remove the label and place the label in a locked shred bin. If the portion of the label containing III remains behind after attempted removal the information should be redacted using a method that renders the information unreadable. Wristbands are placed in locked shred bins. Other non-paper items are placed in the "red" waste management bins for infectious material or the regular trash if they do not contain III when appropriate.
- g. Maintaining Auditory Privacy: Staff only discusses patient care issues in appropriate areas, which allow the maintenance of auditory privacy. Facility staff does not discuss patient information in areas not conducive to confidentiality (e.g., canteen, elevators, or hallways). Signs must be posted alerting Veterans to auditory privacy concerns in waiting areas. VHA health care providers and staff must refrain from discussing patient information within hearing range of anyone who is not on the patient's treatment team or does not have a need to know the specific patient information unless an emergent condition arises whereby auditory privacy cannot be maintained. Administrative staff should follow the same guidance in any discussion involving individually identifiable sensitive information, i.e. employee health or disciplinary actions. Appropriate safeguards include training all staff on auditory privacy to include:
  - 1) Using the Veterans Health Identification Card (VHIC) for identification upon check-in, if available;

- 2) Speak quietly when discussing a patient's condition with the patient or the patient's family members in a public or open area or where the conversation can be overheard such as a waiting room or multi-patient room;
  - 3) Only discussing the information necessary to accomplish the function; for example, not asking for the full Social Security Number (SSN) when the last four of the SSN is sufficient;
  - 4) Asking other Veterans in line for clinical check-in to wait a short distance away from the desk to allow a zone of audible privacy as opposed to being right behind the Veteran being assisted;
  - 5) Only calling Veterans back to an exam room, pharmacy window or other treatment area by name; and
  - 6) Going behind closed doors to have discussions pertaining to the personal information of the Veteran.
- h. Use of Facsimile (Fax): When using fax technology, facility staff adheres to VA Handbook 6500, Information Security Program; VHA Handbook 1907.01, Health Information Management and Health Records; and VHA Directive 1605.01, Privacy and Release of Information.
- 1) III is only transmitted via facsimile (fax) when absolutely necessary. Any disclosure of faxed information containing or requesting individually identifiable patient information must be accounted for in the ROI Plus software or on a electronic spreadsheet provided by the facility Privacy Officer.
  - 2) Any staff member utilizing fax as a means of transferring III must take the following steps to ensure that III is sent to the appropriate destination and not to a machine accessible to the general public:
    - (2.1) Verify the fax number prior to sending the fax and, in order to prevent misdialing, do

not use pre-programmed numbers unless the number is tested prior to faxing. Periodically verify the fax numbers of frequent recipients. Ask those frequent recipients to notify the facility of any fax number changes.

(2.2) A fax cover sheet with an appropriate confidentiality statement, instructing the recipient of the transmission to notify the facility if received in error, must be sent with all outgoing faxes. PHI should never be placed within the fax cover sheet as this negates the confidentiality statement on a fax coversheet. However, the Veteran's name may be referenced in the subject line.

(2.3) For example when transmitting outside VA:

*"This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above."*

(2.4) Notify the recipient before sending the fax in order to ensure that someone is present to receive the information or that the fax machine is in a secure location (e.g. locked room).

(2.5) Review the fax confirmation slip to verify that the confidential information went to the proper destination number. If there has been an error, immediately contact the incorrect recipient and request return or destruction of the fax.



- 3) Electronic mail (e-mail) and information messaging applications and systems are used as outlined in VA policy (VA Directive 6301 and VA Handbook 6500). These types of messages never should contain III, unless the authentication mechanisms have been secured appropriately (see VA Handbook 6500). Responding to a patient via email, which contains protected health information, should be done through My Health eVet Secure Messaging.
- 4) Mailing of Sensitive Information. Mailing of Veteran's correspondences such as copies of records, appointment letters may be done so using the United States Postal Service. Envelopes, parcels, packaging or boxes containing sensitive information must be secured in a manner that prevents unauthorized access, tampering, or accidental loss of contents. Window envelopes must show the recipients' names and addresses, but no other information. (See VA Directive 6609)
- 5) To the extent practicable, this facility mitigates any harmful effect known to have resulted from an improper use or disclosure of III. Mitigation may include, but is not limited to: operational and procedural corrective measures; re-training, reprimanding, or disciplining workforce members; addressing problems with any involved business associates; incorporating the chosen mitigation solution(s) into facility procedures. All employees are responsible for reporting improper uses or disclosures of PHI/PIHI or any other privacy complaint or incident to their supervisor, Privacy Officer, Information System Security Officers, and/or the respective alternate, upon discovery or observation. Staff will report privacy issues to their supervisor or the VA Police Department after-hours or on weekends. If reported to their supervisor, the supervisor is responsible for reporting the privacy issue to the PO/ISSO/Police Department as appropriate. Reporting can occur via encrypted email, telephone or in-person.

## V. Sanctions

- a. All individuals who use or have access to VA information systems or sensitive information must sign and adhere to the Rules of Behavior, which bind them to the legal and moral responsibility of preventing unauthorized disclosure. (See VA Handbook 6500, Information Security Program) This facility has established sanctions, which are applied against members of its workforce as appropriate, for failures to comply with privacy policies and procedures and Rules of Behavior.
- b. This facility has established a set of rules that describes the information privacy operations of the facility and clearly delineates the responsibilities and expected behaviors of all workforce members. These rules address all significant aspects of using III and the consequences of inconsistent behavior or non-compliance. The entire workforce of this facility will have access to a copy of these rules for purposes of review. A signed (manually or electronically) acknowledgement of these rules is necessary for each workforce member.
- c. The facility Privacy Officer will determine information privacy violations and provide evidence thereof. The employee's supervisor will determine appropriate actions and may, in conjunction with human resources management, take necessary steps and apply appropriate sanctions for any employees who are non-compliant with privacy policies and procedures. Penalties will be assessed against any individual(s) who accesses, uses, discloses, or obtains information without the individual's written authorization or not as authorized by law regardless of whether it was an intentional violation or not.
- d. Appropriate legal authorities outside of VHA may levy civil or criminal sanctions for privacy violations. Depending on the statute, penalties range from \$50,000 and/or one year in jail to \$250,000 and/or up to ten years in jail, per offense. If a penalty is levied, the offending employee, not VA, is responsible for payment. In addition, other adverse actions, administrative or disciplinary may be taken against

employees who violate the statutory provisions. Under the HITECH Act, applicable to violations occurring on or after February 18, 2009, the Secretary of Health and Human Services can impose civil monetary penalties for each violation ranging from at least \$100 to a maximum of \$50,000 for the lowest category violation. Under the highest category violation, the Secretary can impose a \$50,000 penalty per violation. Additionally the HITECH Act increases the maximum penalty that the Secretary of HHS can impose for all such violations of the same HIPAA provision in a calendar year from \$25,000 to \$1,500,000.

- e. Appropriate adverse actions must be taken in accordance with VA Directive 5021.

#### VI. Privacy Training and Education

- a. The facility Privacy Officer, in coordination with the facility Education Coordinator or Education Office, is responsible for developing a local-level privacy training policy that outlines the facility procedures for ensuring compliance with the annual privacy training requirement of VHA Directive 1605 and VHA Directive 1605.01.
  - 1) All the members of this facility's workforce receive annual training and education on privacy policies and procedures appropriate for their official functions. All new employees will complete Privacy and HIPAA focused training within 30 days. If they are given access to the Network the privacy training must be completed before Network access is granted. All training is documented in the VA Learning Management System (TMS). For annual mandated trainings, the employee and their supervisor will receive a 30 day notification that a training course is due for completion. If mandatory security training is not completed before the due date the employee's computer access will be removed upon review and direction by the Medical Center Director. Only upon completion of security training is access

restored. Other mandated trainings not completed on time may result in potential personnel action.

- 2) The facility Privacy Officer will conduct privacy training at all facility New Employee Orientation (NEO) programs.
  - 3) Employees are responsible for annual completion of their mandatory privacy training requirement prior to or on their anniversary date of privacy training the following year.
- b. The facility Privacy Officer is responsible for developing a local training strategy in conjunction with the facility Education Coordinator or Education Office. The Privacy Officer presents at New Employee Orientation bi-weekly and conducts annual Privacy Awareness activities during Information Protection Week. The PO will perform weekly facility privacy assessments rounds with the Environment of Care (EOC) team; perform a privacy assessment at night or on the weekend; and assess CBOCs at least once annually to ensure privacy policies are being met and heighten awareness for patient privacy issues. Privacy Officer will ensure bulletins are sent out regarding new privacy information; meet with individual departments during staff meetings; and or conduct activities around the facility, to promote privacy awareness for personnel and to enhance awareness of patient's privacy rights. The health care facility Director will make the strategy available to the VHA Privacy Office upon request.
- c. The facility Privacy Officer, in coordination with the facility Education Coordinator, TMS Coordinator or Education Office, shall maintain a process of compiling annual training records in order to report the facility privacy training completion status to the VHA Privacy Office and to the health care facility Director upon request. TMS reports will be run by the Privacy Officer when requested.
- 1) The annual training records of completion of privacy training must be kept for all workforce members to include the following; employees, volunteers, students, and contractors in order for

reporting of facility privacy training completion numbers by each group.

- 2) The facility Director will certify annual training completion to the VHA Privacy Office for all work force members based on the reports generated by the health care facility Privacy Officer and Education Coordinator, TMS coordinator or Education Office upon request.
- d. The facility Privacy Officer shall conduct other activities within the facility to enhance awareness of privacy and that have a positive impact on the overall privacy culture and posture of the facility. These activities shall include, but are not limited to, participation in VA's annual Privacy Week activities, posting privacy posters and announcements throughout the facility, and conducting one-on-one training with personnel who have been observed displaying negative privacy culture behaviors.

## VII. Privacy Threshold Analysis

- a. The Privacy Threshold Analysis (PTA) is an internal document used by the Privacy Officers, information system owners and the Information System Security Officers (ISSOs). Based on the information in the PTA, Privacy Impact Assessment (PIA) support determines if a PIA is required under the E-Government Act of 2002.
- b. PTAs identify programs and systems that are privacy-sensitive and contain PII. PTAs create an annual record of major system changes and standardize the privacy compliance process. PTAs strengthen the understanding of VA systems, programs, and projects. PTAs are written so that individuals who don't have a technical background can understand what's being stated.
- c. PTA's are to be completed and submitted to the VA Privacy Service PIA support mail group [PIAsupport@va.gov](mailto:PIAsupport@va.gov) on an annual basis unless there is a major change to an IT system prior to the annual review.

- d. The facility Area Manager or designee will review the MAPSCAN notating PII may be provided to the Privacy Officer for comparison with the applicable PTA during the annual review process of completing the PTA on an annual basis. The Area Manager will assign the completion of the PTA for the VISTA and GSS system. Other system PTAs will be assigned to the system owner. After completion the PTA will be submitted to the ISO and PO for review. The Privacy Officer will coordinate the submission to the VA Privacy Office email group PIA support @va.gov for approval and determination whether a PIA will be required. The Privacy Officer will obtain all signatures and return the signed document to the [PIAsupport@va.gov](mailto:PIAsupport@va.gov). When final approval is received the ISSO will upload the document to the designated site.

#### VIII. Privacy Impact Assessment

- a. PIAs outline the risks and effects of collecting, maintaining, and disseminating PII. They mitigate potential privacy risks by evaluating protections, such as security and privacy controls. They can also introduce alternative processes for handling information.
- b. PIAs help identify the overall privacy risk level of a system, program, or project. PIA's inform leadership, program offices, and Veterans about how VA is implementing privacy and mitigating risks associated with PII collection, use, and maintenance.
- c. PIA's are to be completed and submitted to the VA Privacy Services PIA support mail group at [PIAsupport@va.gov](mailto:PIAsupport@va.gov) every three years unless there is a major change to the IT system prior to the three year period.
- d. The Privacy Officer (PO) will notify the OIT Area Manager that a PTA is due for the VISTA and GSS systems. The Area Manager will assign a staff member to complete and forward to the Privacy Officer and ISSO for review. After review the PO will submit the document to the [PIAsupport@va.gov](mailto:PIAsupport@va.gov) email for approval. After approval the PO will obtain all of the

required signatures, save the document as a pdf and send to the [PIAsupport@va.gov](mailto:PIAsupport@va.gov). After approved the ISSO will upload the document to the appropriate site.

#### IX. Personally Identifiable-Information Database Inventory

- a. The facility Privacy Officer, in coordination with the facility CIO, ISSO, Records Manager and facility IT staff shall maintain a process for identifying databases which collect or maintain PII/PHI.
- b. The PO ensures databases identified with PII/PHI are accounted for in existing PTA and PIA.
- c. If the databases identified are not accounted for, then the PO updates the PTA and PIA documents accordingly.
- d. Database inventories are done on an annual basis.
- e. The facility completes an annual database inventory review through a Social Security Number Reduction Spreadsheet and Bio-Medical Inventory List. If further information is required, a MAPSCAN would be requested.

#### B. Individual Rights

##### I. Verification of Identity

- a. In order to receive or view information from his or her VHA record, an individual must present staff with adequate information for verification of identity. Individuals may not verify identity by email.
- b. A Veteran Health Identification Card (VHIC), passport, driver's license, or employee identification card may be used to identify an individual who appears in person. Mail or fax identification requests may be verified by social security number, address and signature comparison to the VHA record.
- c. Whenever possible the facility will verify accuracy of the information in our systems; such as ROI Plus and CPRS, directly with the Veteran during check-in or

- check-out of appointments. Chart reviews of CPRS, ROI Plus, other software or databases will be monitored for accuracy.
- d. This facility shall recognize legally designated personal representatives as the individual when the individual is unavailable or unable to act on his/her own behalf. Staff should recognize the following representatives of the individual:
- 1) **Legal Guardian:** A person designated by a court of competent jurisdiction to manage the property and rights of another person who, due to defect of age, medical condition, understanding, or self-control, is considered by the court to be incapable of administering the individual's own affairs. Depending on the circumstances, the court may appoint a legal guardian for a specific purpose (NOTE: A VA Federal fiduciary is not a legal guardian). Three of the most common types of guardianships are: Legal Guardian of the Person; Legal Guardian of the Property; and Legal Guardian of the Person and Property.
  - 2) **Power of Attorney (POA):** All POA's are to be referred to the Privacy Officer, or the HAS/Release of Information Supervisor for determination that the POA meets the legal requirements for making disclosure decisions.
- e. A personal representative of a deceased individual is a person, who under applicable law, has authority to act on behalf of the deceased individual. This may include power of attorney (if binding upon death), the executor of the estate, or someone under federal, state, local or tribal law with such authority. The next of kin of a deceased individual is considered a personal representative of the deceased individual but not of a living individual. They are recognized as having the same rights as the deceased individual. When there is more than one surviving next-of-kin, the personal representative will be determined based on hierarchy: spouse, adult child, parent, adult sibling, grandparent, or adult grandchild.



**NOTE:** Regardless of the type or source of the POA presented, the reviewer must always carefully check the document with General and Special Powers of Attorney. The document must be: in writing; signed by the individual giving the power; dated; notarized and signed by a licensed notary public; and specifically designate, by name, the third party agent, which may be an organization or entity, to act on behalf of the individual.

## II. Right of Access

- a. If access is legally appropriate, individuals may obtain a copy of, or inspect their record or III. A request to obtain a copy or inspect their record or III must be made in writing by the individual or a personal representative. Individuals may use VA Form 10-5345a, Individuals Request for a Copy of their Own Health Information, to accomplish this purpose.
- b. All requests for copies of individuals' own health information will be directed to HAS/Release of Information. All requests must show date received whether by use of a date stamp, writing date received on request, or entering the request in the ROI Plus software the exact same day as received in person or mail.
  - 1) When an individual requests their Sensitive Patient Access Report (SPAR) and does not give a period of time for the running of the report, the VHA healthcare facility Privacy Officer should ask the individual for the timeframe desired. If the individual wants the SPAR for the entire timeframe for which it exists, then it would be provided as such under Right of Access.
- c. If the individual or the individual's representative is not entitled to the records under any legal provisions, the facility will not provide him or her with a copy of the records. NOTE: this is an infrequent occurrence.
- d. Access to view a record must be processed as follows:

- 1) When individuals appear in person at a VA health care facility, they must be advised at that time whether the right of access or review of records can be granted. When immediate review cannot be granted due to staffing or availability of records, necessary arrangements must be made for a later personal review, or if acceptable to the individual, the copies may be furnished by mail.
- 2) Mailed requests must be referred to the facility Privacy Officer, Release of Information Supervisor, or designee for determination if the right of access by review will be granted.
  - (2.1) If additional information is required before the request can be processed, the individual requesting review of the records must be advised.
  - (2.2) If it is determined that a request to review will be granted, the individual must be advised by mail that access to view the records will be given at a designated location, date and time in the facility, or a copy of the requested record will be provided by mail, if the individual has previously indicated or has been contacted to verify that a copy of the record will be acceptable.
- e. Typically right of access requests, granted requests, denials and adverse determinations are documented in the ROI Plus software, in accordance with VHA Directive 1615, Mandated Utilization of Release of Information (ROI) Plus software. However, the following areas outside of ROI process right of access requests: Employee Health.

### III. Notice of Privacy Practices

- a. An individual will be provided with a copy of IB 10-163, Notice of Privacy Practices, by this facility upon verbal or written request. All Veterans receive a copy of this notice from the Health Eligibility Center (HEC) upon enrollment.

- b. An individual may obtain a copy of IB 10-163, Notice of Privacy Practices, from the Privacy Officer, Release of Information Supervisor or from the privacy office website at [http://vaww.privacy.va.gov/Privacy\\_Publications.asp](http://vaww.privacy.va.gov/Privacy_Publications.asp).
  - 1) A Non-Veteran who receives care and treatment at a facility whether for humanitarian purposes or enrolled in a VA research study must be given a copy of the Notice of Privacy Practices. The Clerk that enrolls the patient into the computer will provide the non-Veteran/Humanitarian with a copy of the NOPP and have them sign the Acknowledgment of the Notice of Privacy Practices form VAF10-0483. The Clerk or the AOD will also notify the Privacy Officer by email of the non-Veteran patient admission/clinic or emergency room visit and scan the signed Acknowledgement for to the non-Veteran's CPRS record. The notification can also include sending the PO a copy of the signed acknowledgement form. The signed acknowledgement for non-Veterans participating in research will be maintained in the protocol file.
  - 2) In an Employee Health situation, an Employee Health staff member may maintain a copy of the acknowledgment form in a binder or in the blue employee health folder if applicable. CPRS should be used only if there is not another place to keep the acknowledgement form.
  - 3) The facility must also establish a process to monitor this requirement to ensure compliance with the rules. Monitoring will be conducted and reported on a quarterly basis.. See VHA Handbook 1605.04 for further information.

#### IV. Amendment Request

- a. An individual has the right to request an amendment to any information or records retrieved by the individual's name or other individually-identifiable information contained in a VA system of records, as provided in 38 CFR 1.579 and 45 CFR 164.526. The right to seek an

amendment of this information or records is a personal right of the individual to whom the record pertains. The personal representative of a deceased individual has a right to request an amendment of the decedent's records. A request for name change is considered an amendment request and must have the appropriate legal documents in order for the Master Veteran Index (MVI) Coordinator to make the change.

- b. The amendment file must be retained and destroyed in accordance with the Record Control Schedule (RCS) 10-1, Privacy Amendment Case File under Section 1005.00 and 1006.9. The amendment files are not scanned into the Veteran's health record as they are not considered part of the health record. They may be maintained in a secure and locked file cabinet or scanned to a secure network drive but cannot be scanned into the administrative portion of VistA Imaging in the health record. The amendment must be maintained for the life of the health record.
- c. The request must be delivered to the Privacy Officer in order for a date to be placed on the request. Requests may be scanned and securely emailed to the PO, interoffice mailed or hand delivery.
- d. Requests to amend records are acknowledged in writing within 10 working days of receipt and if a determination cannot be made within this time period the individual is advised of when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request. All requests will be acknowledged by the Privacy Officer upon receipt.
- e. The Privacy Officer refers the request and related record to the health care provider who authored the information in order for the provider to determine if the record needs to be amended as requested.

- f. When an amendment is approved, the following actions are taken:
- 1) Any information to be deleted must be made illegible, e.g. marked through, in the paper record. For electronic health records, the facility Privacy Officer or Chief, Health Information Management (HIM) is required to use the Computerized Patient Record System (CPRS) Text Integrated Utility (TIU) functions for amending documents. For all other records, the facility Privacy Officer will work with the responsible record custodian to amend their records, e.g. police or employee records.
  - 2) Any new material must be recorded on the original document. The words "Amended-Privacy Act, Amendment Filed, and/or 45 CFR Part 164" must be recorded on the original paper document. The new amending material may be recorded as an addendum if there is insufficient space on the original document. The original document must clearly reflect that there is an addendum and care must be taken to ensure that a copy of the addendum accompanies the copy of the original document whenever it is used or disclosed. The amendment must be authenticated with the date, signature, and title of the person making the amendment.
  - 3) For an electronic amendment of a TIU (Text Integration Utility) document, the Chief of Health Information Management (HIM), or designee, is responsible for utilizing the TIU AMEND action for all TIU documents. Please refer to the TIU User Manual for specific instructions on utilizing the TIU amend functionality found on the HIM website. If the original document cannot be amended and an addendum cannot be attached, then a link to the location of the amendment must be provided. Refer to Non-TIU Document Changes and Corrections Frequently Asked Questions (FAQ) for processes to correct Non-TIU documents.
  - 4) The individual making the request for amendment must be advised in writing that the record has been amended and provided with a copy of the

amended record. The Chief of HIM, or designee, or the facility Privacy Officer, or designee, must notify the individual so that they can identify who they shared their amended health information with and agree to have us notify any relevant persons or organization that had previously received their information. If 38 U.S.C. § 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations, unless the information is disclosed for treatment purposes.

In addition, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must notify all relevant persons or organizations to which the facility disclosed the amended information. If 38 U.S.C. 7332-protected health information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations.

- 5) If the record has been disclosed prior to amendment to a business associate, the business associate must be informed of the correction and provided with a copy of the amended record.
- g. When a request to amend a record is denied, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must promptly notify the individual making the request of the decision. The written notification must:
- 1) Reason for the denial (i.e. information was not created by VHA; information is accurate, relevant, complete or timely in its current form; or information is not part of a VHA system of records or designated record set);
  - 2) Advisement of appeal rights (the individual may appeal to the Office of General Counsel (024), 810 Vermont Avenue N.W. Washington, DC 20420). If the General Counsel sustains the adverse decision, the individual must be advised, in the appeal decision letter, of the right to file a concise

written statement of disagreement with the VA health care facility that made the initial decision.;

- 3) Instruction that if an appeal is not filed, the individual has the right to request the VA Medical Center to provide a copy of the initial request for amendment and the subsequent denial with all future disclosures of information.;
  - 4) Instruction that the individual may also provide a statement of disagreement to the facility and request that the facility provide the statement of disagreement with all future disclosures of the disputed information. A statement of disagreement is to be no longer than two pages in length, an individual may submit a longer statement if it is necessary to set forth the disagreement effectively, however the PO or Chief of HIMS will make the determination to accept it or not;
  - 5) Instruction that the individual may complain about the denial to VHA Privacy Office or to the Secretary, Health and Human Services;
  - 6) The name or title and telephone number of the person or office of contact; and
  - 7) The signature of the facility Director in responding to amendment requests has been delegated to the Privacy Officer.
- h. If requested by the individual, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must identify the individually-identifiable information that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment and the facility's denial of the request to the individual's record.

#### V. Confidential Communications Request

- a. An individual's oral or written request to receive any or all types of communications (correspondence) from facility staff via a confidential alternative means, or at an alternative location, must be processed in

- accordance with VHA Directive 1067, Confidential Communications or subsequent directive.
- b. All confidential communications requests will be referred to the Eligibility Office.
  - c. When the Veteran makes the request of a staff member to allow for the receipt of written communications at an alternative address other than the permanent address of record:
    - 1) Veterans must specify a start date for use of the confidential correspondence address. Dates occurring in the past are not acceptable. Veterans may specify an end date for use of the address, but it is not required.
    - 2) The staff member must access the Load/Edit Patient Data menu option and answer the prompts. VistA allows the capture of the new confidential communications address fields including date started and stopped, street address, city, state, zip code including the four digit geocode, and country.
  - d. If the confidential communications data is on file for the Veteran, that address is used for the mailing of all communications under a specified correspondence type (see VHA Directive 1067, Attachment A, for definitions of the five correspondence types for Health Insurance Portability and Accountability Act (HIPAA) Confidential Communication).
  - e. Requests to split communications under a correspondence type are considered unreasonable and will be denied. With an exception to My HealthVet, a request to receive communications via electronic mail is also to be considered unreasonable and will be denied.
  - f. The confidential communications address and correspondence type is transmitted nightly to the Austin Information Technology Center (AITC).
  - g. A confidential communications address that results in undeliverable mail is considered invalid; and the



correspondence is resent or re-mailed to the Veteran's permanent address as notated in VistA.

- h. When a confidential communications address is activated for health records, the address is viewable through the ROI Plus software for utilization by the ROI Clerks. ROI Clerks must use the confidential communications address when activated to provide individuals with copies of their own records regardless of the address on the request without further communication with the individual and subsequent change within VistA.

## VI. Restriction Request

- a. An individual's requests for restrictions on the use or disclosure of his or her Individually Identifiable Health Information (IIHI) that is used to carry out treatment, payment, or health care operations are referred to the facility Privacy Officer. All restriction requests must be made in writing.
- b. All requests for restrictions of individually identifiable health information need to be reviewed on a case-by-case basis by the facility Privacy Officer. If the facility is considering granting the request, the VHA Privacy Office should be consulted. Restriction requests are not considered unless they meet the following criteria:
  - 1) Submitted in writing;
  - 2) Identify which information is to be restricted;
  - 3) Identify who the information is to be restricted from;
  - 4) Indicate for what purposes (e.g. use for payment) the identified information is to be restricted; and
  - 5) Be signed and dated by the individual to whom the record pertains.

**NOTE:** Although this facility is not required to agree to restrictions requested by individuals on behalf of VHA, any restriction granted must be appropriately

documented. If a request for restriction is granted, all VHA programs and employees must adhere to the restriction unless the information covered by the restriction is needed to provide a patient with emergency treatment.

- c. Restrictions requested by individuals, any restriction granted must be appropriately documented. If a request for restriction is granted, all facility programs and employees must adhere to the restriction unless the information covered by the restriction is needed to provide a patient with emergency treatment. In the rare event that a restriction request is granted, it should be entered into the ROI Plus software under "alerts." This software option is designed to notify facility only Release of Information clerks that certain portions of the Veterans record should not be disclosed. The current treatment team along with other VA personnel should be notified and documented by the Privacy Officer based on the specific access restriction.
- d. When a restriction request is denied, the facility Privacy Officer promptly informs the individual of the decision. The notification includes the reason for the denial and the signature of the facility director or designee. All restriction requests and denials are documented and retained by the Privacy Officer. There are no appeal rights given for a denial of a restriction request.
- e. A facility has a right to terminate a restriction request. A facility may terminate a restriction, if it informs the individual in writing that it is terminating its agreement to a restriction and that such termination is only effective with respect to protected health information created or received after VHA has so informed the individual.

**NOTE:** A facility health care provider may NOT grant a restriction request. A verbal request by the Veteran to not share his/her information is not a restriction request. The provider must refer the Veteran to the Privacy Officer for consideration. The Privacy Officer will send a broadcast email to all providers annually to remind them they may not grant Veteran restriction requests. The Veteran should be informed they need to make their written request to the facility Privacy Officer.

## VII. Facility Directory Opt-Out

- a. Individuals may request exclusion from the Facility Directory during each inpatient admission, in accordance with the Chief Business Office Procedure Guide 1601B.02. The facility Directory Opt-Out provision does not apply to Emergency Rooms unless the patient is going to be admitted to an inpatient setting. The facility Directory Opt-Out provision does not apply to Outpatient clinics.
- b. Upon admission, VistA will prompt the user to select either opt-in or opt-out for each inpatient in the facility directory. During the admission screening process, Registration Staff must ask each inpatient to specify whether he or she wishes to be excluded from the facility directory and document his/her decision in the VistA system at each admission episode.
- c. VistA should be edited utilizing either the Admit a Patient or Extended Bed Control options to indicate the patient's preference.
- d. Each patient must be advised that if they request to be excluded, medical center staff will not be permitted to provide any information to visitors or callers concerning whether a patient is an inpatient at the facility. This includes family, friends, colleagues, deliveries (i.e., flowers, cards, etc.), receipt of mail, or anyone asking about the patient.
- e. A patient may, at any time during an admission, change the initial decision to be included or excluded from the facility directory.
- f. If an inquiry is received concerning a patient who elects to opt-out of the facility directory, the sample response may be "I am sorry, but I do not have any information I can give you on whether John Q. Veteran is a patient." This includes deliveries such as flowers, cards, etc. All staff including telephone operators, volunteers, mail delivery staff and Ward staff must be familiar with this process. This restriction does not apply to communications that are part of the treatment, payment

or health care operations or if other legal authority allows for the disclosure of patient's health information.

- g. If the patient is incapacitated or unable to make this decision at the time of admission, the facility health care provider admitting the patient makes a determination based on the patient's prior admissions and the best interest of the patient.
  - 1) The provider must document this decision in the patient's medical record in CPRS.
  - 2) Once the patient is able to communicate or make the facility directory opt-out decision, the patient must be given an opportunity to do so. The clinical staff member who elicits the patient's decision to opt-out or not opt-out when the patient is able to communicate will enter a note into the medical record and notify the Admitting staff to make the change in VistA.
  - 3) The Privacy Officer discusses this top during New Employee Orientation. All Staff and Providers receive annual privacy training which includes discussion of the Opt-Out process. Privacy Officer will provide additional training as appropriate from results of Opt-Out monitoring.

#### VIII. Accounting of Disclosures

- a. The facility maintains an accounting of all disclosures of III for six (6) years after the date of disclosure or for the life of the record, whichever is longer. (See RCS10-1 for additional guidance or your Records Control Officer) This accounting includes disclosures made with or without patient authorization. Disclosures of data to VHA employees performing their official duties in regards to treatment, payment and health care operations and disclosures of de-identified data do not require an accounting as well as traditional FOIA requests, or to an individual under the Right of Access provision or disclosures of a limited data set or de-identified data or for VHA use of individually-identifiable health information.

- b. In most circumstances, the accounting will be maintained electronically via the most current version of the ROI Plus software as part of the record from which the disclosure was made. See VHA Directive 1615, Mandated Utilization of the Release of (ROI) Plus software.
- c. For those departments within the VA health care facility that do not utilize the ROI Plus software either a CPRS note or excel spreadsheet will be utilized. Prosthetic Services VA Form 10-2319 will be generated when a request is received. Office of Community Care currently uses the software REFDOC2.2. A progress note State Prescription Drug Monitoring Program will be used for accessing the Texas State Prescription Drug Monitoring Application. The Infection Control department utilizes TheraDoc application to document their reporting.
- d. An individual may request a copy of an accounting of disclosures from his/her records. The request must be made in writing, and adequately identify the system of records or designated record set(s) for which the accounting is requested. The request must be delivered to the facility Privacy Officer so that a date can be put on the request for processing and completion within the 60 calendar days.
- e. Accountings must contain the name of the individual to whom the information pertains, date of each disclosure; the nature or description of the disclosed information; a brief statement of the purpose of each disclosure, or in lieu of such statement, a copy of a written request for each disclosure; and the name and, if known, address of the person or agency to whom the disclosure was made.
- f. The accounting of disclosure must be made available within 60 calendar days of the facility's receipt of the request, except for disclosures made for health oversight activities or law enforcement purposes authorized by 38 C.F.R. §1.576(b)(7) and 45 C.F.R. §164.528(a)(2)(i).

- 1) If the accounting cannot be provided within the specified timeframe, the timeframe may be extended 30 days.
- 2) In order to extend the timeframe, the requestor must be issued a written statement from the facility Privacy Officer that includes the reasons for the delay and the date by which the accounting will be provided. Only one such extension of time for action on a request for an accounting of disclosures is permitted.

### **C. Uses and Disclosures**

#### **I. Minimum Necessary**

- a. The minimum necessary requirements do not apply to disclosures to, or requests by, a health care provider who requires the information for treatment purposes.
- b. All facility staff should have minimum necessary (for completion of job duties) access to PHI. Specific minimum necessary policies and procedures, including appropriate staff access levels, are explained in VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information.
  - 1) The functional categories for each employee shall be assigned upon new hire and reviewed annually during performance appraisals and/or annual competence assessment reviews by employee's immediate supervisor based on VHA Handbook 1605.02, Appendix B. The Supervisor will advise employees of their functional category (or categories) to carry out their assigned job duties. Employee's signature will signify their acknowledgement. All residents, interns and affiliated students will be apprised of their functional status when completing their Mandatory Training for Trainees (MTT) Rules of Behavior.
  - 2) Employee's access to PHI will be determined by the employee's position description and in turn, their menu access to VistA. If PHI access is granted, the employee's supervisor must determine their functional category. Supervisors, with input from the facility Privacy Officer (as

needed) determine which category and access to PHI for each employee to perform their duties.

## II. Authorizations

- a. The facility does not use or disclose III without appropriate authority conferred by applicable federal privacy laws and regulations or individual written authorization. Valid authorizations are used only for the purpose(s) stated in the authorization and only disclosed by or released to the personnel or office listed in the authorization.
- b. A written authorization signed by the individual to whom the health information or information pertains is required when:
  - 1) The facility needs to use III for a purpose other than treatment, payment, and/or health care operations, and other legal authority does not exist; and
  - 2) The facility discloses information for any purpose for which other legal authority does not exist.
- c. An authorization to release information must be made in writing and include the following information:
  - 1) The identity (i.e., full name, date of birth and last four of the social security number for scanning purposes) of the individual to whom the information pertains.
- d. A description, which identifies the information in a specific and meaningful fashion, of the information to be used or disclosed.
- e. The name of the person(s) or office(s) authorized to make the requested use or disclosure.
- f. The name or other specific identification of the person(s) or office(s) to which the agency may make the requested use or disclosure.

- g. A description of the purpose(s) for the requested use or disclosure. A statement “insurance purposes” etc., is sufficient. A purpose is not required when disclosing the information to the individual to whom the information pertains.
- h. An expiration date, condition or event that relates to the individual or the purpose of the use or disclosure of the information. If the purpose section is not filled out and there is no expiration date, condition or event, the authorization is considered invalid. Examples of appropriate expiration date language specific to research are:
  - 1) The “end of research study”, or similar language, is sufficient if the authorization is for use or disclosure of III for research.
  - 2) The statement “none” or similar language is sufficient if the authorization is for the agency to use or disclose III for a research database or research repository. The statement “none” cannot be used as an expiration date for any purpose other than research.
- i. The signature of the individual, or someone with the authority to act on behalf of the individual, the date of the signature must be included on the authorization.
- j. A statement that the individual has the right to revoke the authorization in writing except to the extent that this facility has already acted in reliance on it, and a description of how the individual may revoke the authorization.
- k. A statement that VHA, this facility, or the entity requesting the information may not condition treatment, payment, enrollment, or eligibility for benefits on the individual’s completion of an authorization. NOTE: This statement is only required if the requestor is another HIPAA covered entity.
- l. A statement that III disclosed in response to the authorization may no longer be protected by federal laws or regulations and may be subject to re-disclosure by the recipient.



- m. When an authorization is received by MEDVA MC or it's CBOCs for patient records the request will be sent to the Release of Information Department for processing.
- n. Authorization may be given:
  - 1) On VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information, or any subsequent authorization form approved to replace this form or a specific authorization developed for a specific VA program, e.g. eHealth Exchange.
  - 2) Using an outside entity's authorization form (e.g., Social Security Administration Authorization form) as long as all of the authorization content requirements are met.
- o. Information will not be disclosed on the basis of an authorization form that:
  - 1) Fails to meet all the preceding requirements;
  - 2) Has expired;
  - 3) Is known to have been revoked;
  - 4) Has been combined with another document to create an inappropriate compound authorization; or
  - 5) That is known, or in the exercise of reasonable care should be known, to facility staff as false with respect to any item of the authorization requirements.
  - 6) Release of Information staff will handle an authorization that is invalid and consult with the Release of Information Supervisor or Privacy Officer when authorization may be questionable.

Authorizations for documents protected by 38  
U.S.C. §7332:

- a. Testing for HIV and Sickle Cell Anemia are no longer considered protected conditions therefore they can be disclosed without an authorization.
- b. Veteran Request: If 38 U.S.C. §7332-protected health information is to be disclosed for any purpose other than treatment, this information must be specifically identified by checking the boxes.
- c. Facility staff will not check off any of the 38 U.S.C. §7332 boxes on the VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information, unless the individual is specifically asked in person while a clerk completes the form for the individual prior to signing or a telephone discussion with the individual before mailing the authorization for signature. Staff may not arbitrarily check-off boxes without the individual's oral approval. Oral approval is documented by annotating the discussion with date and time of discussion under "internal comments" within the ROI Plus software. The cover letter submitted to the individual with the enclosed VAF 10-5345 for signature and return may also denote the telephone conversation or verifying signature within scanned documents.
- d. If the authorization indicates specific 38 U.S.C. §7332-protected health information is to be released to include future health information with a future expiration date but the Veteran does not have the indicated 38 U.S.C. §7332-protected diagnosis at the time of signature, the authorization is considered to be invalid for any future 38 U.S.C. §7332-protected information acquired after the signature. This newly acquired §7332-protected information cannot be disclosed without a new authorization being obtained. Marking all boxes on VA Form 10-5345 for 38 U.S.C. §7332-protected health information

when the Veteran only has one is not an acceptable practice. If the Veteran marks all 38 U.S.C. §7332 boxes and does not have the diagnoses AND this authorization is for a one time use, then the authorization is still valid.

Release of USC 7332 for the purpose of treatment:

The patient may check the box indicating that they do not want 7332 information released for the purpose of this authorization however, in accordance with VA Mission Act, Public Law 115-182 on June 6, 2018, 38 U.S.C. 7332 was amended to permit disclosures to non-VA entities for purpose of providing health care to patients relating to HIV, sickle cell anemia and substance abuse without a signed, written authorization from the patient.

- p. Producing and Using Video, photographs, audio or voice recordings:
  - 1) In accordance with VHA Directive, 1078, VA Form 10-3203, Consent for Production and Use of Verbal or Written Statements, Photographs, Digital Images, and/or Video or Audio Recordings by VA must be used when VHA is producing or using images.
  - 2) In accordance e with VHA Directive , 1078 VA Form 10-3203a Informed Consent and Authorization for Third Parties to Produce or Record Statements, Photographs, Digital Images or Video or Audio recordings by VA must be used when VHA is agreeing to a third pary interviewing an individual.
- 2) VHA must also obtain an authorization from the patient or personal representative using VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information, **prior to disclosing** for official purposes a photograph, digital image, or video or audio recording if the product contains individually identifiable health information or protected health information. Refer to VHA Directive 1078,

Privacy of Persons Regarding Photographs Digital Images and Video or Audio Recordings, for additional guidance.

III. Processing a Request for Release of Information

- a. Anyone may request VHA to disclose any record. Any request for information maintained in VHA and facility records must be processed under all applicable confidentiality statutes and regulations.
- b. A request for copies of facility records must be in writing, under the signature of the requestor, and describe the record(s) sought, so it may be located in a reasonable amount of time.
- c. All written requests for copies of individually identifiable health information maintained within the facility will be forwarded to the ROI Department except as indicated below. The facility Privacy Officer will be consulted on any requests received that are unusual or are not addressed in this policy.
  - 1) The Medical Care Cost Recovery (MCCR) Coordinator, or equivalent, is responsible for disclosing billing information. MCCR staff is also responsible for coordinating with Release of Information staff in order to account for disclosures of health information.
  - 2) Disclosures of PHI/IIHI by any other service or individuals other than the Release of Information Department is not allowed without appropriate legal authority. An Accounting of Disclosure (AOD) must be created by the releasing department and provided to the Privacy Officer upon request. An AOD of these disclosures is performed quarterly by the Privacy Officer through spot checks.
- d. The ROI Department will need to determine who is making the request for a copy of the facility record or information.
  - 1) If the requestor is the individual to whom the records pertain, follow the guidance under B. Individuals Rights, 2.0 Right of Access.

- 2) If the requestor is other than the individual to whom the record pertains (third party), determine what information or record is requested and for what purpose and is there a written valid authorization from the individual or other legal authority prior to disclosure.
- e. The ROI Department will determine what information is being requested.
- 1) If the record requested does not contain individually identifiable information, process the request in accordance with section D. Freedom of Information Act.
  - 2) If the record requested contains individually identifiable information, review the paragraphs under C. Uses and Disclosures, 4.0 Uses/ Disclosures for Treatment, Payment, and Health Care Operations, and Other Operations Not Requiring Authorization for guidance directed at the specific requestor and/or purpose.
  - 3) If the record requested contains individually identifiable information and the guidance in section C. Uses and Disclosures, 4.0 Uses/ Disclosures for Treatment, Payment, and Health Care Operations, and Other Operations Not Requiring Authorization is not applicable and a signed, written authorization was not received, refer the request to the facility Privacy Officer for an opinion. The facility Privacy Officer will review the request and determine if disclosure authority exists by reviewing the applicable Federal privacy laws and regulations.
  - 4) If the request is on a deceased individual, process the request in accordance with section C. Uses and Disclosures, 5.0 Deceased Individuals.
- f. The ROI Department must process requests for individually identifiable information within specified time standards and charge the applicable fees, as appropriate.

- 1) Requests for copies of individually identifiable information must be answered within 20 workdays from the date of receipt.
  - 2) When, for good cause shown, the information cannot be provided within 20 workdays from the date the request was initially received, the requester must be informed in writing as to the reason the information cannot be provided and the anticipated date the information will be available.
  - 3) Copying fees may be charged for copies of records provided to requestors. Only copying fees as stated in 38 C.F.R. §1.577(f) or subsequent regulations may be charged. The facility is prohibited for charging more for copies than is allowed in VA regulations.
- g. A requestor may ask that the facility disclose or provide individually identifiable information in an electronic format, such as on Compact Disk (CD), in lieu of paper copies. When the records requested exist electronically and can be reproduced in the requested format, the facility must accommodate such a request. The ROI Department will work with IRM when records are requested in an electronic format. When records are requested in an electronic format the ROI staff will respond to the request by burning the requested information onto a CD.

#### IV. Uses/Disclosures for Treatment, Payment, and Health Care Operations, and Other Operations Not Requiring Authorization

- a. This facility uses and discloses IIHI as permitted by the HIPAA Privacy Rule, the Privacy Act of 1974 and other federal rules and regulations. Certain disclosures, within VA, for purposes other than treatment, payment, and health care operations, may be made without authorization. If disclosure includes information protected by 38 U.S.C. §7332, Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus, or Sickle Cell Anemia express written authorization by the patient may be required.

- b. Individuals are not required to and cannot be forced to waive their rights under the HIPAA Privacy Rule, 45 C.F.R. §160.306 as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.
- c. The facility workforce (e.g. staff, employees, volunteers) uses and discloses IIHI in the following manners:
  - 1) Within VHA on a need to know basis for treatment, payment, and/or health care operations without the written authorization of the individual.
  - 2) To the extent necessary, on a need-to-know basis, and in accordance with good medical and/or ethical practices, staff may disclose general patient information to the patient's next-of-kin. If the patient is listed in the facility directory, staff also may disclose to the general public, without authorization, the patient's location and general condition.
  - 3) To next-of-kin and family members:
    - (3.1) In the presence of the individual if the patient does not object or if it is reasonably inferred from the circumstances that the patient does not object. Specific verbal consent is required by the patient to discuss information protected by U.S.C. 7332
    - (3.2) Outside the presence of the individual in the professional judgment of attending medical center staff members, disclosure is in the best interest of the patient excluding information protected by U.S.C. 7332
  - 4) To VBA for use in the determination of eligibility for, or entitlement to, benefits.
  - 5) To VA contractors or business associates for a contracted service or service provided on behalf of the facility related to treatment, payment, and/or health care operations provided that the disclosure is within the scope of the contract or agreement

and when necessary, a signed BAA with the contracted company or business associate is on file.

- 6) To a receiving facility when a patient is transferred to, or being treated at a community hospital (including other federal hospitals).
- 7) If a referral is made to another non-VA facility, State Veterans Home or a community nursing home information may be shared without an authorization from the individual.
- 8) To the Office of Resolution Management (ORM) when necessary for determining compliance with Equal Employment Opportunity (EEO) requirements and upon the request of the Office of Resolution Management.
- 9) To the Board of Veterans Appeals for benefits, including the processing and adjudication of claims appeals.
- 10) To the National Cemetery Administration for determinations of eligibility for, or entitlement to, benefits.
- 11) To VA Unions, in the course of fulfilling their representational responsibilities. VA Unions may make a request to management for copies of facility records pursuant to its authority under 5 U.S.C. § 7114(b) (4). Unions may request any records that are maintained by a VA facility. For example, this might include releasable portions of completed Administrative Investigation Boards (AIB), patient medical records and/or an employee's personnel records. However, under certain circumstances, unions may not be legally entitled to receive IIHI, or information protected by other statutes such as the Privacy Act. All requests for information submitted by VA Union Representatives are referred to the servicing HRMS, which coordinates the response with the District Counsel and the facility Privacy Officer (designee) and/or the facility FOIA Officer (designee).



- 12) To a Member of Congress (including a staff member acting on the Member's behalf) when responding to an inquiry from a Congressional office that is made at the request of the individual to whom the information pertains. VHA may disclose individually-identifiable information, excluding 38 U.S.C. 7332-protected information, to a member of Congress or staffer in response to an inquiry made pursuant to a constituent request. The request from the congressional office must be in writing and signed. The request for information should also include a copy of the constituent's inquiry to the Congressman unless a signed, written authorization is provided.

If a prior written authorization is provided by the constituent, it must conform to the requirements of a valid authorization. If the request is not the result of an inquiry made on behalf of the individual's family or another third party. VAMC staff cannot provide information to a Congressional member if the inquiry was initiated by a family member or person other than the individual to whom the information pertains.

- (12.1) If the constituent's inquiry is from the personal representative of the individual to whom the information pertains, VHA will require a Power of Attorney, guardianship document, or some other document that demonstrates that the requester is authorized under Federal, State, local or tribal law to act on behalf of the individual. If the constituent cannot be identified with reasonable certainty with the information provided, VHA may request additional information before the request is processed.

- (12.2) Before disclosing any information to a member of Congress, the request must contain the elements outlined in VHA Directive 1605.01, paragraph 18.

Congressional requests are referred to the Director's Office for processing.

- d. To health insurance carriers or health plans for payment activities related to seeking reimbursement for VA care. Effective June 6, 2018, with the enactment of the VA Mission Act of 2018, P.L. 115-182, there is now legal authority to make this disclosure pursuant to 38 U.S.C. § 7332(b)(2)(I). VA does NOT have to obtain an authorization from the patient to submit the bill/claim or to provide copies of medical records to support the bill/claim.
- e. To General Counsel and/or District Counsel for the purposes of health care operations, e.g. legal services, as long as a business associate agreement is in effect. In addition, information may be provided to the Office of General Counsel (OGC) for any official purpose authorized by law as long as VHA Central Office maintains a MOU or BAA with OGC authorizing the sharing of IIHI for legal counsel provided to VHA.
- f. Except for criminal law enforcement activities, to the VA Inspector General or Office of Inspector General (OIG) Investigators for any official purpose authorized by law, such as health care oversight.
- g. Except for criminal law enforcement activities, to the facility VA Police for enforcement of physical security (e.g., escort of high-risk patients).
- h. To the VA Office of Employment Discrimination, Complaints, and Adjudication (OEDCA) to review the merits of employment discrimination claims filed by present and former VA employees and non-agency applicants for employment.
- i. To the VHA Office of Medical Inspector (OMI) to address health care problems to monitor and improve the quality of care provided by VHA.
- j. To the United States Office of Special Counsel (OSC). The U.S. Office of Special Counsel (OSC) is an independent agency that enforces Whistleblower protections, safeguards the merit system and provides a secure channel for whistle blower disclosures.

- k. VA Human Resources Management Services (HRMS). VHA may disclose individually-identifiable information to VA HRMS as authorized by law. There is no authority under the HIPAA Privacy Rule for the disclosure of a VA employee Veterans' health record to management or personnel officials for disciplinary investigation purposes without prior signed, written authorization from the employee.
- l. American Red Cross. VHA may disclose the nature of the patient's illness, probable prognosis, estimated life expectancy and need for the presence of the related active duty Service member to the American Red Cross, for the purpose of justifying emergency leave of the active duty Service member. Information protected by 38 U.S.C. 7332 may not be disclosed for this purpose.
- m. Bureau of Census VHA may disclose individually-identifiable information, excluding 38 U.S.C. 7332-protected information, to the Bureau of Census for purposes of planning or carrying out a census or survey or related activity (see HIPAA Privacy Rule 164.512(a) and 5 U.S.C. 552a(b)(4)).
- n. TRICARE. VHA may disclose 38 U.S.C. 7332-protected information to DoD (TRICARE) without written authorization from active duty personnel for treatment or payment purposes.
- o. Military Command legal authority exists for VHA to make the disclosure of a patient's protected health information to the military commanding officer without an authorization if:
  - 1) The patient is a member of the Armed Forces;
  - 2) The requester is a military command authority; and the purpose for which the health information is requested is required to meet the military mission.

Relevant health care information may be disclosed to Department of Defense (DoD), or its components, for individuals treated under 38 U.S.C. 8111A for the purposes deemed necessary by appropriate military

command authorities to assure proper execution of the military mission.

- p. Whistleblower is a member of the VA workforce or VHA business associate, who reasonably believes that VHA has engaged in conduct that is unlawful or otherwise violates professional or clinical standards or that the care, services, or conditions provided by VHA potentially endangers one or more patients, workers, or the public, may always disclose protected health information to VA OIG and Congressional Committees (e.g., House Veterans Affairs Committee and Senate Veterans Affairs Committee) authorized by law to investigate or otherwise oversee the relevant conduct or conditions of VHA. NOTE: Individual members of Congress are not covered.

A whistleblower may disclose any protected health information, except information protected by 38 U.S.C. 7332 (HIV, Sickle Cell, Drug and Alcohol Treatment) to OSC, a public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of VHA, or an appropriate healthcare accreditation organization with whom VHA has a relationship, such as The Joint Commission, for the purpose of reporting the allegation of failure to meet professional standards or misconduct by VHA.

An employee who discloses protected health information to an entity other than those listed above may be considered to have made an unauthorized disclosure in violation of the Privacy Act, 38 U.S.C. 7332, HIPAA Privacy Rule or VHA policy. Such unauthorized disclosure may result in disciplinary action.

- q. Veterans Health Information Exchange (VHIE) [formerly named VLER]:  
The health information shared is a pre-determined standards-based set of clinical data that is sent to the requester through the Exchange. Direct access to the Veteran's health record is not involved or authorized; only requested information is exchanged via a virtual architecture with the non-VA health care provider who has an established treatment relationship with the Veteran. Veterans will automatically be opted-in for the

Exchange but may opt-out or request restrictions of non-VA participant organizations by filing standard VA Forms online or at their closest VA Medical Center's Release of Information (ROI) Office.

- r. Requests from Courts and Quasi-Judicial Bodies: Disclosure must be in accordance with VHA Directive 1605.01 and requests from Courts and Quasi-Judicial Bodies should be referred to the facility Privacy Officer who will consult with legal counsel as necessary.
- s. VA Researchers.
  - 1) VHA may use employee information, including health information for official VHA research studies, in accordance with VHA Directive 1200, Veterans Health Administration Research and Development Program, other applicable 1200 handbook series, and 38 CFR Part 16.
  - 2) For use or disclosure of individually-identifiable health information involving non-employee research subjects for research purposes (see paragraph 13, Research).
  - 3) If the research involves pictures or voice recordings for other than treatment purposes, the Informed Consent (10-0086) must state that a photograph, image or video/audio recording is going to be made. If the documentation of ICF is waived, the script for the audio-recording must include the subject's permission to be recorded.

**NOTE:** Use of a patient's photograph or voice for purposes other than the identification, diagnosis, or treatment of the patient is not permitted unless a signed consent is obtained on VA Form 10-3203, Consent for Production and use of Verbal or Written Statements, Photographs, Digital Images, and/or Video or Audio Recordings by VA (38 C.F.R. §1.218). If photographs are taken to support treatment, those photographs are included in the health record maintained for each patient and do not require VAF 10-3203. Disclosure of the patient's photograph or voice would require written authorization on VAF 10-5345 from the

individual or personal representative. (See VHA Directive 1078(1), Privacy of Persons Regarding Photography, Digital Images and Video or Audio Recording).

- t. The Privacy Officer will be contacted to assist in coordination of disclosures to the Veteran or third-party requestors.

V. Deceased Individuals

- a. Except for uses and disclosures for research purposes discussed in section C. Uses and Disclosures, 10.0 Research Activities; this facility shall protect the PHI of a deceased individual in the same manner, and to the same extent, as required for the PHI of living individuals.
- b. PHI, excluding 38 U.S.C. §7332-protected health information, of a deceased individual may be disclosed to coroners, medical examiners, and funeral directors. Title 38 U.S.C. §7332-protected health information may be disclosed for determining cause of death or required for collection of death or vital statistics per State law.
- c. Disclosure of autopsy findings:
  - 1) The Diagnostic Service Line Manager is responsible for preparing the autopsy provisional diagnoses report and ensuring its availability to the attending physician; for disclosing pathology/tissue slides/blocks; for releasing radiographic films and for following up to ensure return of this VA property and coordinating with Release of Information to account for the disclosure.
  - 2) Managers of Clinical Service Lines are responsible for translating autopsy findings into layman's terms and composing a timely autopsy letter in lay terminology upon request.
  - 3) A copy of the autopsy clinical finding summary and the listing of clinical-pathological diagnoses on Standard Form (SF) 503, Medical Record-Autopsy Protocol, are disclosed, when requested by the next-of-kin.

- 4) All cases in which the autopsy reveals drug abuse, alcoholism or alcohol abuse, HIV infection, or sickle cell anemia information (which is subject to additional disclosure restrictions), the autopsy results are not disclosed to the next-of-kin unless the facility Privacy Officer has determined that such disclosure is necessary for the survivor to receive benefits.

## VI. Contracts and Business Associate Agreements

- a. In contracts/agreements that involve the use or disclosure of PHI, appropriate privacy requirements, specifications, and statements of work must state that privacy requirements and specifications should be properly implemented before the contract/agreement goes into operation.
- b. All contracts must meet the contracting requirements dictated by VA's Office of Acquisition and Material Management and the Federal Acquisitions Regulations (FAR). Any contract which necessitates the use of III must conform to the policies and procedures in FAR Subpart 24.1, Protection of Individual Privacy and VA Directive 6500.6, Contract Security.
- c. The contracting officer, the Privacy Officer, and the ISSO will work together to identify those entities that qualify as Business Associates under HIPAA and ensure that BAAs are enacted for these identified entities in accordance with HIPAA and BAA policies and procedures (NOTE: a business associate relationship exists if the facility is required to release PHI to a contractor or business partner for the provision of services on the facility's behalf.)
- d. All contracts, agreements, and relationships must be assessed to determine if a business associate relationship exists.
- e. If a business associate relationship is determined to exist, a business associate agreement is enacted utilizing only the most current version of the VHA Health Information Access Office approved BAA language available at

<http://vaww.vhadatportal.med.va.gov/PolicyAgreements/BusinessAssociateAgreements.aspx>.

- f. If a business associate is determined to serve more than one VA facility, the facility Privacy Officer should contact the VHA Health Information Access ([hia.va.gov](http://hia.va.gov)) mail group to discuss enacting a national BAA. Any national BAA takes precedence over a local BAA. Local and regional BAAs should not be initiated if a national BAA exists for the same services as described in the national BAA preamble. BAAs are kept updated and documented as long as the agreement is in force. (Refer to VHA Handbook 1605.05, Business Associate Agreements)
- g. Per the agreement, business associates will abide by the terms and conditions spelled out in the agreement.
- h. If a pattern of activity or practice of the business associate constitutes a material breach or violation of the business associate's obligation under the contract or other agreement is discovered, the facility Privacy Officer reports the problem to CSOC and works with the Contracting Officer for resolution. All Business Associates must report the breach within 24 hours to the Director of Health Information Governance and submit a written report within 10 days.
- i. The Contracting Officer's Representative (COR) responsible for the contract will monitor compliance with the applicable privacy policies required under the Business Associate Agreement with assistance and in consultation with the facility Privacy Officer.

## VII. Emergency Situations and Serious and Imminent Threats

- a. When an employee becomes aware of a threat to the patient, another individual (e.g. family of veteran) or to the public, the VAMC staff should contact the facility Privacy Officer in order to determine if, and how, to report or address the serious and imminent threat to the health or safety of the patient, other individual or public.
- b. VHA may disclose individually-identifiable information, excluding health information, to law enforcement



agencies (e.g. Federal, State, local and/or Tribal authorities) charged with the protection of the public health for reporting a serious threat to the health and safety of an individual or the public without a standing written request letter or written request if upon such disclosure notification is transmitted to the last known address of the individual to whom the information pertains.

- c. When a local law enforcement agency approaches VAMC staff to obtain health information on a Veteran or patient due to a current or ongoing serious and imminent threat to the public, the facility Privacy Officer and VA Police should be contacted. During regular business hours, the facility Privacy Officer will make the disclosure of requested health information to the law enforcement officials in a position to prevent or lessen the threat. Such disclosure should be made immediately once the facility is made aware of the serious and imminent threat. If health information is needed after hours, the Administrative Officer of the Day (AOD) or other facility personnel designated to address emergent facility issues after hours should be contacted by VA Police to assist local law enforcement officials in obtaining information to lessen or prevent the threat.
- d. VHA may disclose IIHI, excluding 38 U.S.C. §7332-protected health information, in accordance with:
  - 1) 5 U.S.C. §552a(b)(8)- to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if, upon such disclosure, notification is transmitted to the last known address of the individual to whom the records pertain; and
  - 2) 45 C.F.R. § 164.512(j)(1)(i)- to avert a serious and imminent threat to the safety of an individual as long as the disclosure is made to a party which is in a position to prevent or lessen the threat, such as a law enforcement official or the individual threatened; or
  - 3) 45 C.F.R. § 164.512(k)(2)- to avert serious threats to the safety of the public as long as the PHI is

given to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, or other national security activities.

**NOTE:** This disclosure requires an accounting of disclosure through the ROI Plus software. Also, a notification letter must be sent to the person to whom the health information pertains. The person has a right to know who received their information and what information was disclosed by VHA.

#### VIII. Standing Written Request Letters

- a. VHA may disclose IIHI protected information pursuant to a valid standing written request letter to State Agencies charged with the protection of the safety and health of the public. Information disclosed in response to a standing written request letter is provided for the purpose of cooperating with a State law enforcement reporting requirement. District Counsel will be consulted to determine if State laws would allow for standing written request letter to be implemented.
- b. Standing written request letters may be needed for the following purposes:
  - 1) Law Enforcement- Law enforcement entities routinely require reporting from VHA records for suspected child abuse, suspected elder abuse, gunshot wounds, and other administrative actions, e.g., suspension or revocation of a driver's license.
  - 2) Public Health- Examples of public health reporting requiring a standing written request letter include:
    - (2.1) Communicable diseases (e.g., hepatitis, tuberculosis, sexually transmitted diseases, etc.);
    - (2.2) Vital statistics (e.g., deaths, etc.); and
    - (2.3) Other State reporting requirements (e.g., animal bites).
  - 3) State and Other Public Registries (e.g. State Cancer Registries, NOTE: VHA may not disclose

individually-identifiable information to private registries without the prior written authorization of the individual to whom the information pertains.)

- 4) Coroner or Medical Examiner
- c. With the exception of public health reporting requirement defined in VHA Directive 2013-008, Infectious Disease Reporting, all other disclosures are discretionary on behalf of the facility.

The facility Privacy Officer has oversight of the standing written request letter process and is responsible for ensuring all standing written request letters meet the guidelines as defined in 1605.01 (21)b. A standing written request letter is good for a period of 3 years and after which it must be renewed. A copy of all standing written request letters must be maintained by the facility Privacy Officer for 5 years after the standing written request letter has expired.

- d. The Privacy Officer is responsible for obtaining, maintaining and renewal of all valid standing written request letters on file. The Privacy Officer will maintain a copy of the written and signed Standing Letter from the state agencies. At this time standing letters are on file for reporting to Adult and Child Protective Services, Cancer Registry and the State Department of Health.
- e. Departments responsible for disclosing information pursuant to a valid standing written request letter must coordinate the disclosure with the Release of Information Department or Privacy Officer in order to account for the disclosure.
- f. If a standing letter is not in place the party requesting the IHI must submit a written request under the authority of 5 U.S.C. 552a(b)(7) for the information. The request must be:
  - 1) In writing;
  - 2) Specify the particular portion of the record desired;
  - 3) Specify the law enforcement activity or purpose for which the record is sought;

- 4) State that de-identified data could not reasonably be used; and
- 5) Be signed by the head of the agency.

IX. State Prescription Drug Monitoring Program

- a. VHA may disclose individually-identifiable health information to a State Prescription Drug Monitoring Program (SPDMP) without the signed, written authorization of the Veteran for whom the medication was prescribed. Disclosure may be for the purpose of querying the SPDMP or reporting mandatory prescription information to the State (e.g., batch reporting).

**NOTE:** Batch reporting is currently available. Please work with your local IT and Pharmacy departments to ensure appropriate use and functionality of the process.

- 1) A progress note has been created for providers to use when accessing the SPDMP.
- 2) A note in CPRS can be used to account for the SPDMP query disclosures; however, the Chief of HIM should be involved in the development of the note template.

X. De-identification of PHI

- a. Information is only considered de-identified if the methods outlined in VHA Directive 1605.01 are followed. Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual **and** if VHA has no reasonable basis to believe it can be used to identify an individual. This is accomplished by either
  - 1) having an expert with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information could be used, alone or in combination with other

reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and documents the methods and results of the analysis that justify such determination; or

- 2) all eighteen (18) identifiers listed in VHA Directive 1605.01 are removed.
- b. De-identified data is not PHI. Therefore, when data is appropriately de-identified, the HIPAA Privacy Rule, the Privacy Act and other federal privacy regulations do not apply and information may be disclosed under the Freedom of Information Act.
- c. VA Directive 6511 Presentations Displaying Personally Identifiable Information must be followed prior to presenting at VA and non-VA conferences. The presentation will be submitted to the Privacy Officer for review when appropriate.

XI. Research Activities: General

- a. VA Research investigators must have appropriate legal authority to collect, access, or use individually identifiable information in a research study. The “need-to-know” in their official performance of their job duty does not cover all federal privacy regulations specific to research.
- b. The facility Privacy Officer and the facility Information System Security Officer (ISSO) will serve in non-voting capacities on the R&D Committee pursuant to VHA Handbook 1200.05 Requirements for the Protection of Human Subjects in Research.
- c. The facility Privacy Officer will review all initial submissions of human subject research protocols, including exempt protocol submissions, for the use and/or disclosure of individually identifiable information and other privacy considerations prior to the convened Institutional Review Board Meeting (IRB) at which the study is to be reviewed, except for those research projects approved by the VA Central IRB. It is expected that review submissions and approval process will be timely submitted by all parties involved. The

Information System Security Officer (ISSO) will review all initial submissions of human subject research protocols for compliance with all applicable federal security requirements. The Privacy Officer and the Information System Security Officer (ISSO) will provide a final written summary to the IRB. The Privacy Officer's final written summary must include approval of the HIPAA Authorization and validation that the IRB appropriately approved the waiver of HIPAA Authorization as appropriate prior to the use and/or disclosure of III by the researcher or his/her team.

- d. The facility Privacy Officer and Information System Security Officer (ISSO) will review all continuing reviews of human subject protocols or proposed human subject protocol amendments impacting privacy or information security. The application BRAIN is used by both the PO and ISO to document their review and approval of submitted protocols. In addition, the PO will complete VA Form 0250 and provide to the R&D Committee for inclusion in the research file.
- e. Facility research office staff verifies the qualifications of VA researchers seeking to use and/or disclose III, (i.e. they have completed their mandatory privacy and security training) and ensures that the VA researchers take appropriate measures to protect the privacy of study subjects.

XII. Research Activities: Use

- a. VA Research investigators may use III for reviews preparatory to VA research, provided that the information is being sought solely for purposes preparatory to research and that no PHI will be removed by the VA researcher. All other requirements related to the use of III for reviews preparatory to VA research are set forth in VHA Handbook 1200.05; Requirements for Protection of Human Subjects Research must be followed.
- b. VA Research investigators may use PHI for VA-approved research if the facility Privacy Officer has determined that:

- 1) A Research HIPAA authorization compliant with VHA Directive 1605.01 Para. 14 will be obtained for each research subject; or
  - 2) The IRB has approved a waiver of HIPAA authorization, in full or in part, and the IRB approval has been appropriately documented as required by the HIPAA Privacy Rule and VHA Handbook 1200.05; or
  - 3) A Limited Data Set will be used and a valid DUA has been signed as required by the HIPAA Privacy Rule.
- c. If the researcher has not completed his or her study by the time of the expiration of the Research HIPAA authorization, the researcher can no longer use any of the information previously collected from the study subjects.
- d. PHI/III and other VA sensitive data for a VA-approved research study that is stored, collected, or maintained outside of VA custody, either electronic or paper must have prior approval and safeguards in place to protect the data. The facility Privacy Officer will work with the facility Information System Security Officer (ISSO) and Area Manager to ensure the appropriate safeguards are in place. See VA Handbook 6500 for further guidance.
- e. For certain sensitive research studies, a VA researcher may request a Certificate of Confidentiality from the National Institutes of Health (NIH) which, if granted could prevent the facility from being forced to disclose individually identifiable information on research subjects, by a court order/subpoena in any civil, criminal, administrative, legislative, or other proceedings that are maintained in 34VA12, Veteran, Patient, Employee, and Volunteer Research and Development Project Records.

### XIII. Research Activities: Disclosure

- a. For the facility to disclose protected health information to a non-VA researcher or other non-VA entity for research purposes, either for VA research purposes, or for non-VA research programs, there must be legal

authority under all applicable federal privacy laws and regulations including 38 U.S.C. § 5701, the Privacy Act, HIPAA Privacy Rule and 38 U.S.C. §7332. The applicable legal authority is as follows:

- 1) 38 U.S.C. § 5702 – If the non-VA researcher or non-VA entity is requesting III, that may be disclosed under 38 U.S.C. § 5701, a written request stating records sought and purpose of the records that is dated and signed by the non-VA researcher is required. If VA is initiating the disclosure of information under 38 U.S.C. § 5701 for a research purpose, a written request from the non-VA researcher or non-VA entity is not required.
- 2) 38 U.S.C. § 5701 – For purposes of disclosing records pertaining to any claim under any of the laws administered by the Secretary for non-VA Research, a “federal” non-VA researcher may be provided name and address of individuals under 38 U.S.C. § 5701(b)(3). For a “non-federal” researcher or other entity, the researcher or entity must provide to VA the names and addresses of the individual whose claims information is being sought in order to obtain those individuals’ identifiable information.
- 3) 38 U.S.C. §7332 – The non-VA researcher to whom 38 U.S.C. §7332-protected health information (related to drug abuse, alcoholism, or alcohol abuse, infection with the human immunodeficiency virus, or sickle cell anemia) is disclosed must provide written assurance that the purpose of the data is to conduct scientific research and that no personnel involved in the study may identify, directly or indirectly, an individual patient or subject in any report of such research or otherwise disclose patient or subject identities in any manner. This assurance may be documented in the research protocol. In addition, the Medical Center Director based on input from the ACOS, Research and Development must determine that the non-VA researcher is qualified to conduct the research; has a research protocol that stipulates how the information will be



maintained in a secure manner; and a written statement that the research protocol has been reviewed by an IRB who found that the individual's rights are adequately protected and that the potential benefits of the research outweigh any potential risks to patient confidentiality.

**NOTE:** If a VA researcher plans to disclose 38 U.S.C. §7332-protected health information to an outside non-VA entity or use within a publication, this written assurance must also be obtained.

- 4) Privacy Act of 1974 – If an individual does not provide prior written consent for the disclosure of his/her record contained in a system of records (SOR), there must be a routine use under the applicable Privacy Act System of Records that permits the disclosure. (See 34VA12, Routine Use 19)
- 5) HIPAA Privacy Rule – Either a research HIPAA authorization compliant with VHA Directive 1605.01 Para. 14 will be obtained for each research subject; or the IRB has approved a waiver of HIPAA authorization and the IRB approval has been appropriately documented as required by the HIPAA Privacy Rule and VHA Handbook 1200.05.

**NOTE:** A waiver of HIPAA authorization approved by the IRB does not affect or override the other legal requirements that must be met.

- b. A VA researcher must have appropriate legal authority to disclose individually identifiable information to a non-VA entity, including a research sponsor or an academic affiliate who is collaborating on this study. This disclosure authority is outlined in the written HIPAA authorization signed by the individual unless other legal authority exists, e.g., Court Order.
- c. Decedents' information may be disclosed to a source other than the researcher who has use of this data if the HIPAA Privacy Rule allows for disclosure to a non-VA entity. See your facility Privacy Officer in regards to any questions concerning disclosure authority.

- d. This facility may distribute a limited data set, information that excludes direct identifiers, but still contains potentially identifying information, without consent of the individual. A limited data set is only protected under the HIPAA Privacy Rule as the data is not considered identifiable for purposes of the Privacy Act and 38 U.S.C. §7332. Disclosure of a limited data set is dependent upon the receipt of a DUA, which must:
- 1) Establish the permitted uses and disclosures of the information;
  - 2) Establish who is permitted to use or receive the data set; and
  - 3) Provide that the data set recipient:
    - (3.1) Does not use for further disclose the information other than as permitted;
    - (3.2) Uses appropriate safeguards to prevent improper use or disclosure of the information;
    - (3.3) Reports to the facility/VHA any improper use or disclosure of which it becomes aware;
    - (3.4) Ensures that any agents to whom it provides the data set agrees to the same restrictions and conditions that apply to the data set recipient; and
    - (3.5) Does not identify the information or contact the individuals.
- e. A contracted entity involved in VA research is not a business associate of the covered entity and no business associate agreement is required.
- f. A research disclosure made pursuant to a signed, written research HIPAA authorization to a non-VA entity (study monitor, sponsor, academic affiliate, or other non-VA entities) who is not a research team member or

contractor requires an accounting of disclosure to be maintained. The accounting of disclosure may be maintained concurrently or be created retrospectively from the VA researcher's files. See above Section B, Individual's Rights, 8.0 Accounting of Disclosures.

- g. Facility will not disclose any personal information about VHA personnel engaged in animal research in response to a FOIA request if the FOIA Officer determines a risk to the facility or research personnel.

**NOTE:** Further guidance on Research requirements is available in VHA Directive 1605.01, VHA Handbook 1081.01 Data Use Agreements, VHA Directive 1200, and other applicable 1200 series handbooks.

#### XIV. Logbooks

- a. Unnecessary collection of sensitive personal information (SPI) in physical logbooks is prohibited.
- b. Electronic log books may be maintained with appropriate safeguards in place. **No paper log books may be kept unless there is a mandatory regulation that requires the physical log book.** Use of an unapproved physical logbook will be considered a privacy violation.

### D. Freedom of Information Act (FOIA)

#### I. General

- a. The FOIA, Title 5 United States Code (U.S.C.) 552, implemented by Title 38 Code of Federal Regulations (CFR), Sections 1.550-1.562 provides that any person has the right to obtain access to federal agency records, except to the extent that such records or portions of them are protected from public disclosure by one of the nine FOIA exemptions or by one of three special law enforcement record exclusions.
- b. The FOIA requires disclosure of reasonably described VA records, or a reasonably segregable portion of the records, to any person upon written request, unless one or more of the nine exemptions apply to the records.

- c. A FOIA request may be made by any person (including foreign citizens), partnerships, corporations, associations, and foreign, State, or local governments with some exceptions. The following types of request are not proper FOIA requests:
  - 1) Requests for records by Federal agencies and their employees acting in their official capacity.
  - 2) Requests for records by fugitives from justice seeking records related to their fugitive status.
- d. VHA administrative records not retrieved by name, social security number, or other identifier must be made available to the greatest extent possible in keeping with the spirit and intent of the FOIA.
- e. Before releasing records in response to a FOIA request, the records must be reviewed by the facility FOIA Officer to determine if all or only portions of the records can be released. Portions that cannot be released will be redacted in accordance with the nine exemptions provided in the FOIA. The process of deleting portions of documents before releasing them is referred to as "redaction."
- f. The FOIA mandates that all FOIA requests, absent unusual or exceptional circumstances, be processed within 20 business days of receipt.
- g. To foster ongoing communication and awareness on matters of significant importance to VA and VHA leadership, the facility FOIA Officer must provide notification of substantial interest FOIA requests. A substantial interest FOIA Request is a request for information in which there has been or is likely to generate substantial public interest. This would include, but is not limited to, the following types of requests, regardless of the requester: (1) those related to a threat to the public health; (2) high profile local or national incidents or situations involving VA beneficiaries, employees or officials; and (3) incidents involving an alleged breach of the public trust (e.g., waste, fraud or abuse). The PO will email notification that a substantial interest FOIA request has been received. The facility FOIA Officer will notify the VHA

FOIA Office of all substantial interest FOIA requests following the current procedure set forth by the VHA FOIA Office.

## II. Requests for Copies of Records

- a. Records or information customarily furnished to the public in the regular course of the performance of official duties (e.g., information posted on VAMC Internet site) may be furnished without a written request. If the information sought is available on a VA or VHA public website, a MEDVA MC employee may provide the website address to the requester to avoid having the individual submit a FOIA request for the records.
- b. Requests from individuals for information about themselves, which is retrieved by their names or other personal identifiers, are to be processed as outlined in section B. Individual's Rights, 2.0 Right of Access, unless the Privacy Act system of records maintaining the requested records has been exempted from a first party right of access. First party requests for records from such exempted Privacy Act systems of records will be processed under the FOIA.
- c. A FOIA request may be submitted through any mail service, by facsimile or electronically to an official FOIA mailbox established for the purpose of the receiving FOIA requests. Requests for MEDVA MC records may be submitted to the facility's electronic FOIA mailbox at [vhahoufoia@va.gov](mailto:vhahoufoia@va.gov) or faxed to 713-383-1907 or mailed to MEDVA MC 2002 Holcombe Blvd 00A-PO, Houston, Texas 77030.
- d. Requests for VHA records processed under the FOIA must be in writing and describe the records in enough detail so that they may be located with a reasonable amount of effort. If a request, regardless of the method in which the request was received (i.e., mail, facsimile or e-mail), concerns documents involving a personal privacy interest or are protected by another confidentiality statute, the request must contain an image of the requester's handwritten signature. This procedure cannot be waived for reasons of public interest, simplicity, or speed.

- e. The request does not have to be designated a FOIA request in order for the request to be processed as a FOIA request and the individual seeking the documents does not have to explain why access to agency records is desired.

### III. Processing a FOIA Request

- a. Any MEDVA MC employee receiving a written request for records must be promptly forwarded to the request to the facility's FOIA Officer for action.
- b. Immediately upon receipt of a FOIA request, the facility FOIA Officer will date stamp the request.
- c. All FOIA requests will be entered into the Department of Veterans Affairs' electronic FOIA tracking system.
- d. The facility FOIA Officer will review the request to determine if the request is made in compliance with the FOIA and VA's regulations implementing the FOIA, if the requester is seeking a fee waiver or expedited processing, if the request meets the definition of a substantial interest FOIA request, and if the request was sent to the correct agency component.
- e. FOIA requests not submitted to the correct agency component will be promptly referred by the facility FOIA Officer to the correct component for processing.
- f. The facility FOIA Officer will address requests for fee waivers and expedited processing in accordance with the FOIA.
- g. Substantial interest FOIA request notifications will be completed in accordance local and national procedures.
- h. The facility FOIA Officer shall charge for processing requests under the FOIA in accordance with the FOIA and the VA implementing regulations.
- i. Within ten business days of receipt of the FOIA request, the facility FOIA Officer will acknowledge receipt of the request by sending the FOIA requester an acknowledgement letter.

- 1) The acknowledgment letters to the FOIA requestor will contain the following information:
  - (1.1) the date of the request,
  - (1.2) the date the FOIA Officer received the FOIA request
  - (1.3) a description of the records sought
  - (1.4) the processing track type, e.g. simple, complex, or expedited
  - (1.5) the cut-off date of the records search,
  - (1.6) the assigned FOIA request tracking number,
  - (1.7) the name and contact information of the MEDVA MC FOIA Officer handling the request
- j. A reasonable search for records responsive to the FOIA request will be conducted by the MEDVA MC employees. All records responsive to a FOIA request will be forwarded to the facility's FOIA Officer for processing.
- k. In instances where the FOIA requester fails to provide enough information to locate the requested records, the FOIA Officer will seek clarification from the FOIA requester.
- l. In unusual circumstances, the facility FOIA Officer may extend the 20-business day time limit to process FOIA request an extra 10 business days. The FOIA Officer will notify the requester of the unusual circumstances, that a time extension has been taken, and the date which a response is expected to be issued. If the extension is more than 10 business days, the FOIA Officer will inform the requester of this in writing and provide the requester an opportunity to narrow the scope of the request or arrange for an alternate timeframe.

- m. The facility FOIA Officer will respond to FOIA requestors' inquiries and questions in a timely way and keep the requestor informed during delays in processing.
- n. After making a release determination, the facility FOIA Officer will issue an initial agency decision (IAD) to the requester. The IAD must contain the following information:
  - 1) the date of the request;
  - 2) the date the FOIA Officer received the request,
  - 3) the description of the records sought,
  - 4) the assigned FOIA request tracking number ,
  - 5) the procedural history of the request;
  - 6) the cut-off date of the record search;
  - 7) the exemption(s) cited when information is being redacted or withheld; and
  - 8) the type of information being redacted or withheld (i.e. name, SSN, address, etc.), and,
  - 9) if any adverse determinations are made, the right to appeal to the Office of General Counsel (OGC).
- o. IADs for FOIA requests denied in whole or part must be signed by the Medical Center Director or designee. The Medical Center Director has delegated signature authority to the FOIA Officer for all responses.
- p. FOIA administrative case files will be maintained in accordance with RCS 10-1 and the National Archives and Records Administration (NARA) General Records Schedule and contain the following information:
  - 1) copy of the FOIA request,
  - 2) evidence demonstrating that the FOIA Officer conducted a thorough search for responsive records,



- 3) un-redacted copies of responsive records,
- 4) redacted copies of responsive records sent to the FOIA requestor, and
- 5) Copies of all correspondence, including the signed IAD letter, and contact with requesters and in the case of exemption 4, the submitter, to include, but not limited to emails and letters concerning acknowledgement, fees, scope, clarification, pre-disclosure notification, notice of intent and the initial agency decision.

**NOTE:** Refer to VHA Directive 1605.01 Privacy and Release of Information paragraph 32, and Freedom of Information Act for additional information on processing FOIA requests.

#### IV. Coordination with District Counsel and VHA FOIA Officer

- a. The facility FOIA Officer will consult with District Counsel, VISN, and the VHA FOIA Office concerning FOIA legal requirements and the handling of specific FOIA requests.
- b. In any case where a FOIA request involves matters or subjects involved in ongoing or anticipated litigation, administrative proceedings, or criminal or civil investigation, health care facility personnel must coordinate the facility's response to the FOIA request with their District Counsel.
- c.. If a request involves matters pertaining to ongoing litigation, the District Counsel must be informed of the request to ensure coordination of the VA's position in the litigation with any release of documents.

#### V. Annual Report of Compliance with FOIA

- a. The FOIA requires each agency to complete an annual FOIA report. The facility FOIA Officer must ensure that all requests required for the annual FOIA report are properly entered into the VA's electronic FOIA tracking system to allow for an accurate reporting on the annual FOIA report.

**6. RESCISSION**

Medical Center Policy Memorandum No. 138S-012, *Radiation Safety Program*, dated June 1, 2017.

**7. REVIEW**

Five-year review period at recertification

**8. RECERTIFICATION**

This MCP is scheduled for recertification on or before June 1, 2025. This MCP will continue to serve as local policy until it is recertified or rescinded. In the event of contradiction with national policy, the national policy supersedes and controls.

**9. SIGNATORY AUTHORITY**

FRANCISCO VAZQUEZ, MBA  
Medical Center Director

**ATTACHMENTS:**

Appendix I: Glossary of Terms  
Appendix II: Acronyms

NOTE: The signature remains valid until rescinded by an appropriate administrative action.

DISTRIBUTION: MCPs are available at:

<https://dvagov.sharepoint.com/sites/VHAhou/qsv/DocLib/Shared%20Documents/Forms/Expanded%20Library.aspx>

## APPENDIX I: Glossary of Terms

**Access** means the ability or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

**Availability** means that data or information is accessible and useable upon demand by an authorized person.

**Business Associate** is an entity, including an individual, company, or organization that performs or assists in the performance of a function or activity on behalf of VHA that involves the creation, receiving, maintenance or transmission of PHI, or that provides to or for VHA certain services as specified in the Privacy Rule that involve the disclosure of PHI by VHA.

**Computer matching** describes the computerized comparison of records from two or more automated systems of records. For more information contact the VHA Privacy Office.

**Confidentiality** means that property, data, or information is not made available or disclosed to unauthorized persons or processes.

**De-identified information** is health information that is presumed not to identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual because the 18 Patient Identifiers described in the HIPAA Privacy Rule have been removed. De-identified information is no longer covered by the Privacy Act, 38 U.S.C. § 5701, 38 U.S.C. § 7332, or the HIPAA Privacy Rule.

**Disclosure** refers to the release, transfer, provision of access to, or divulging in any other manner information outside VHA. Once information is disclosed VHA may retain ownership of the data such as to a Business Associate, contract or other written agreement. There are some cases in which VHA may relinquish ownership of the information. The exception to this definition is when the term is used in the phrase "accounting of".

**Electronic media** means:

- (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the

information being exchanged did not exist in electronic form before the transmission.

**Health care operations** mean any of the following activities of the covered entity to the extent that the activities are related to covered functions:

- (1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- (2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- (3) Underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);
- (4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- (5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and,
- (6) Business management and general administrative activities of the entity, including, but not limited to management activities relating to implementation of and compliance with the HIPAA requirements; customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer; resolution

of internal grievances; creating de-identified health information or a limited data set; and fundraising for the benefit of the covered entity.

**Health Information** is any information, whether oral or recorded in any form or medium, created or received by a health care provider, health plan, public health authority, employer, life insurers, school or university, or health care clearinghouse or health plan that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual. This encompasses information pertaining to examination, medical history, diagnosis, and findings or treatment, including laboratory examinations, X-rays, microscopic slides, photographs, and prescriptions.

**Individual** means the person who is the subject of protected health information.

**Individually Identifiable Information (III)** is any information pertaining to an individual that is retrieved by the individual's name or other unique identifier, as well as Individually Identifiable Health Information regardless of how it is retrieved. Individually Identifiable Information is a subset of Personally Identifiable Information and is protected by the Privacy Act.

**Individually identifiable health information** is a subset of health information, including demographic information collected from an individual, that:

- (1) Is created or received by a health care provider, health plan, or health care clearinghouse (e.g., a HIPAA-covered entity, such as VHA);
- (2) Relates to the past, present, or future physical or mental condition of an individual, or provision of or payment for health care to an individual; and
- (3) Identifies the individual or where a reasonable basis exists to believe the information can be used to identify the individual.

**Limited Data Set** is protected health information from which certain specified direct identifiers of the individuals and their relatives, household members, and employers have been removed. These identifiers include name, address (other than town or city, state, or zip code), phone number, fax number, e-mail address, Social Security Number (SSN), medical record number, health plan number, account number, certificate and/or license numbers, vehicle identification, device identifiers, web universal resource locators (URL), internet protocol (IP) address numbers, biometric identifiers, and full-face photographic images. The two patient identifiers that can be used are dates and postal address information that is limited to town or city, State or zip code. Thus, a Limited Data Set is not De-identified Information, and it is covered by the HIPAA Privacy Rule. A Limited Data Set may be

used and disclosed for research, health care operations, and public health purposes pursuant to a Data Use Agreement.

**Non-identifiable Information** is information from which all Unique Identifiers have been removed so that the information is no longer protected under the Privacy Act, 38 U.S.C. §5701, or 38 U.S.C. § 7332. However, Non-identifiable Information has not necessarily been de-identified and may still be covered by the HIPAA Privacy Rule unless all 18 Patient Identifiers listed in the Rule's de-identification standards are removed.

**Patient identifiers** are the 18 data elements attributed to an individual under the HIPAA Privacy Rule that must be removed from health information for it to be de-identified and no longer covered by the Rule.

**Payment** Except as prohibited under 45 CFR §164.502(a)(5)(i), payment is an activity undertaken by a health plan to obtain premiums, to determine its responsibility for coverage, or to provide reimbursement for the provision of health care including eligibility, enrollment, and authorization for services. It includes activities undertaken by a health care provider to obtain reimbursement for the provision of health care including pre-certification and utilization review. **NOTE:** *VHA is both a health plan and a health care provider.*

**Personally Identifiable Information** Personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII elements includes but not limited to: name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc

**NOTE:** The term "Personally Identifiable Information" is synonymous and interchangeable with "Sensitive Personal Information."

**Protected Health Information (PHI)** The HIPAA Privacy Rule defines PHI as Individually Identifiable Health Information transmitted or maintained in any form or medium by a covered entity, such as VHA.

**NOTE:** VHA uses the term protected health information to define information that is covered by HIPAA but, unlike individually-identifiable health information, may or may not be covered by the Privacy Act or Title 38 confidentiality statutes. In addition, PHI excludes employment records held by VHA in its role as an employer.

**Right of access** is an individual's right to have access to (e.g., look at, view) or obtain a copy of records pertaining to the individual that contain individually-identifiable information.

**Sensitive Personal Information (SPI)** is the term, with respect to an individual, means any information about the individual maintained by VA, including the following: (i) education, financial transactions, medical history, and criminal or employment history; and (ii) information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. SPI is a subset of VA Sensitive Information/Data.

**NOTE:** The term "Sensitive Personal Information" is synonymous and interchangeable with "Personally Identifiable Information."

**Subcontractor** A subcontractor is a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

**System of records** refers to any group of records under the control of the Department from which a record is retrieved by personal identifier such as the name of the individual, number, symbol, or other unique retriever assigned to the individual.

**Treatment** is the provision, coordination, or management of health care or related services by one or more health care providers. This includes the coordination of health care by a health care provider with a third-party, consultation between providers relating to a patient, and the referral of a patient for health care from one health care provider to another.

**Unique Identifier** is an individual's name, address, social security number, or some other identifying number, symbol, or code assigned only to that individual (e.g., medical record number and claim number). If these identifiers are removed, then the information is no longer Individually Identifiable Information and is no longer covered by the Privacy Act, 38 U.S.C. § 5701, or 38 U.S.C. § 7332. However, if the information was originally Individually Identifiable Health Information, then it would still be covered by the HIPAA Privacy Rule unless all 18 Patient Identifiers listed in the de-identification standard have been removed.

**NOTE:** The VA Office of General Counsel has indicated that the first initial of last name and last four of the social security number (e.g., A2222) is not a unique identifier; therefore, inclusion of this number by itself does not make the information identifiable or sensitive.

**Use** is the sharing, employment, application, utilization examination, or analysis of information within VHA.

**VA Sensitive Information/Data** is all Department information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifies an individual but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

**Workforce member** means on-site or remotely located employees, contractors, students, WOC, volunteers, and any other appointed workforce members.



## **APPENDIX II: Acronyms**

ADPAC: Automated Data Processing Application Coordination

ADUSH: Assistant Deputy Under Secretary for Health

AIB: Administrative Investigation Board

AITC: Austin Information Technology Center

AOD: Administrative Officer of the Day

BAA: Business Associate Agreement

CCA: confidential communications address

C.F.R.: Code of Federal Regulations

CMS: Centers for Medicare and Medicaid Services

COR: Contracting Officer Representative

CPRS: Computerized Patient Record System

DUA: Data Use Agreement

EEO: Equal Employment Opportunity

FOIA: Freedom of Information Act

HHS: Department of Health and Human Services

HIPAA: Health Insurance Portability and Accountability Act

HRMS: Human Resources Management Service

IIHI: Individually Identifiable Health Information

III: Individually Identifiable Information

IRB: Institutional Review Board

ISSO: Information System Security Officer

IT: Information Technology

MCCR: Medical Care Cost Recovery

MOU: Memorandum of Understanding

OCIS: Office of Cyber and Information Security

OCR: Office for Civil Rights

ODR: Office of District Counsel

OGC: Office of General Counsel

OIG: Office of the Inspector General

ORM: Office of Resolution Management

PA: Privacy Act

PHI: Protected Health Information

PO: Privacy Officer

POA: Power of Attorney

PSETS: Privacy and Security Event Tracking System

QM: Quality Management

R&D: Research and Development

RCS: Records Control Schedule

ROI: Release of Information

TIU: Text Integrated Utilities

U.S.C.: United States Code

VA: Department of Veterans Affairs

VAMC: Veterans Affairs Medical Center

VHA: Veterans Health Administration

VHACO: Veterans Health Administration Central Office

VHIC: Veteran Health Identification Card

VIReC: VA Information Resource Center

VISN: Veterans Integrated Service Network

VistA: Veterans Health Information Systems and Technology Architecture

VSSC: VHA Support Service Center

MICHAEL E. DEBAKEY VA MEDICAL CENTER  
HOUSTON, TEXAS

MEDICAL CENTER POLICY  
MEMORANDUM NO. 00Q-023

December 6, 2019

**JUST CULTURE PRINCIPLES AND CULTURE OF SAFETY**

1. **PURPOSE**

- A. The purpose of this policy is to establish policy and procedures that define the philosophy, expectations, and requirements for Just Culture and to ensure a culture of safety. The Michael E. Debakey VA Medical Center (MEDVAMC) embraces the principles of a Just Culture and fosters a culture of safety. Just Culture ensures balanced accountability for both individuals and the organization responsible for designing and improving systems in the workplace. Principles of Just Culture align with high-reliability, the Blueprint for Excellence and ICARE values that encourage psychological safety, employee self-disclosure and a continual delivery of high-quality services for Veterans, employees, and the community we serve.
- B. The purpose of this policy is to ensure an environment at MEDVAMC where employees feel safe to speak-up and speak-out about reporting of adverse events, near misses, and the existence of hazardous conditions without the fear of retribution or retaliation creating an environment of psychological safety. Psychological safety describes the collective belief of staff, employees and leaders respond to reporting errors, adverse events, near misses, or raise difficult issues and creates learning opportunities for improvements in patient safety. MEDVAMC encourages all employees to identify systems changes and behavior changes, which have the potential to help detect and avoid future adverse events and harm.

2. **POLICY**

It is the policy of MEDVAMC to acknowledge that patient safety events are not commonly the result of individual misconduct (reckless behavior), but rather system or process failures (human error/at-risk behavior influenced by the system as designed). Managers hold positions of authority and power, thus their influence on psychological safety is profound. Supervisors, managers and leaders are responsible for proactively ensuring strong processes, encouraging personnel to report mistakes, assisting with identifying the potential for error, and even stopping work in acute situations. Supervisors, and managers are also responsible for assuring that reported events and near misses are handled consistently and fairly. Employees are accountable for their clinical decision making, behavior choices, and following established guidelines, policies and procedures that ensure safety. Improving

patient safety reduces risk by its focus on managing human behavior (or helping others to manage their own behavior) and redesigning systems.

### 3. **DEFINITIONS**

A. **Just Culture:** A fair and just culture means giving constructive feedback and critical analysis in skillful ways, conducting assessments that are based on facts and having respect for the complexity of the situation. It also means leaders provide fair minded treatment, have productive conversations, and create effective structures that help people reveal their errors and help the organization learn from them. A fair and just culture does not mean non-accountable, nor does it mean an avoidance of critique or assessment of competence. Rather, after careful collection of facts, substandard performance is revealed, and/or there is reckless or willful violation of policies or negligent behavior, corrective or disciplinary action may be appropriate. It is also recognized that employees must balance personal and organizational values with:

- The duty to avoid causing unjustified risk or harm.
- The duty to follow a procedural rule.
- The duty to produce a high-quality outcome.

To this end, MEDVAMC believes in a consistent, fair, and systematic approach to managing behaviors that facilitate a culture that balances a non-punitive learning environment with the equally important need to hold persons accountable for their behavior.

B. **Collective Mindfulness:** A term used to describe a culture of safety.

It is an environment in which all workers look for, and report, small problems or unsafe conditions before they pose a substantial risk to the organization when they are easy to fix.

C. **Safety Event:** A safety event is any variance inconsistent with the desired, normal, or usual operations of the organization.

- (a) Safety events involving patients regardless of whether injury occurs will be reported to Patient Safety and into the Joint Patient Safety Reporting system (JPSR).
- (b) Safety events involving employees should be reported through the DBRS.
- (c) Safety events involving visitors should be reported to the VA Police. VA Police will contact Safety Service.

D. **High Reliability:** High-Reliability organizations (HROs) are those that exist in such hazardous environments where the consequences of errors are high, but the occurrence of error is extremely low. To function in a “collective mindset”, in which all staff look for, and report,

small problems or unsafe conditions before they pose a substantial risk to the organization.

- E. **Psychological Safety:** Psychological safety is the degree to which team members feel that their environment is supportive, trying new ways of doing things, and learning from mistakes. In psychologically safe teams, team members feel accepted and respected. Psychological safety describes the collective belief of staff, employees and leaders response to reporting errors, adverse events, near misses, or raise difficult issues and create learning opportunities for improvements in patient safety.

#### 4. **PROCEDURES**

- A. All employees will use the JPSR system to report patient safety events.
- B. As part of the normal investigative process for any safety event, the Supervisor/Manager will conduct an investigation to determine the type of behavior that led to the safety event and to distinguish between blameworthy and blameless actions. The safety event will be assessed objectively and analyzed using a systematic approach based on three classifications of behaviors/actions:
- a. Human Error
  - b. At-Risk Behavior
  - c. Reckless Behavior

Exceptions to this approach will occur if an individual knowingly or willingly conceals a safety event, hinders a safety investigation, or willfully causes a safety event or commits an unsafe act. In such case, Human Resources will be involved.

- C. The practice for all employees includes:
- a. Reporting a patient safety event as soon as possible (same days as the event) after taking appropriate immediate action.
  - b. Formal reporting will be done using the JPSR reporting system.
  - c. If an employee believes he or she has been subjected to inappropriate punitive measures as a result of self-disclosure, the individual should report this concern to their service leadership, if appropriate, or to Human Resources Management.
- D. Staff will:
- a. Avoid causing unjustified risk or harm (e.g., physical, financial, reputation, privacy, emotional). Be mindful of and look for the risks and hazards around every work situation.
  - b. Report errors and hazards (speak up).

- c. Help to design safe systems.
- d. Manage safe choices:
  - i. Follow procedures
  - ii. Make choices aligned with personal responsibilities and organizational values

E. Supervisors will:

- a. Take proactive measures to ensure their employees understand that the system's culture promotes full disclosure of safety threats or events.
- b. Establish that reported events will be handled consistently with the system's philosophy of responding with a focus on process, prevention and process improvement measures (versus punitive actions).
- c. Promote mutual trust, a just culture atmosphere, encourage staff to speak up, report events and promote patient safety.

Supervisors shall not participate in any form of harassment, intimidation or retaliation against staff or employees for reporting safety events. Intimidating and disrespectful behaviors disrupt the culture of safety and prevent collaboration, communication, and teamwork, which are required for safe and highly reliable patient care. Examples include but are not limited to:

- Inappropriate words (profane, insulting, intimidating, demeaning, humiliating, or abusive language)
- Shaming others for negative outcomes
- Unjustified negative comments or complaints about another provider's care
- Refusal to comply with known and generally accepted practice standards.
- Not working collaboratively or cooperatively with other members of the interdisciplinary team
- Creating rigid or inflexible barriers to requests for assistance or cooperation
- Not responding to requests for assistance or information, such as not returning pages or calls promptly

F. Investigation of Events

- a. Upon formal notification of a safety event, operational leadership associated with the event will begin an investigation process to identify the type of behavior that led to the safety event. These three behaviors/actions are:

- i. **Human Error**- slip lapse or mistake; unintended error and a product of a current system design that often fails to consider the impact of the human factor.
  - ii. **At-Risk** - A choice: risk not recognized, risk of deviation deemed minimal or believed justified.
  - iii. **Reckless** - Intentionally risk taking; knows risk associated with action but consciously disregard risk.
- b. In accordance with applicable significant event or risk management guidelines, managers, senior leaders and other healthcare team members may be notified depending on the severity of the concern or event.

G. Managers will:

- a. Know and understand the risks:
  - i. Investigate the source of errors and at-risk behaviors.
  - ii. Turn events into an understanding of risk.
- b. Design safe systems.
- c. Facilitate safe choices focused on managing behaviors:
  - i. **Human Error** – Consoling (e.g., providing emotional support, and/or crisis management team appropriate to the situation).
  - ii. **At-Risk** – Coaching (e.g., education, review of applicable standards, manage incentives).
  - iii. **Reckless** – Corrective action.
- d. Use the National Center for Patient Safety (NCPS) Just Culture Decision Support Tool (JCDST) (Attachment A) to identify the type of behavior that led to the safety event and determine the appropriate management response. The NCPS JCDST is a tool intended to aid in determining the right course of action when an employee has made an error, drifted into an at-risk behavior, or has otherwise not met his/her obligations to the organization.
- e. Address repetitive patient safety problems, whether caused by individual error or system weakness.
- f. Managers will follow *MEDVAMC Memorandum 05-002 Disciplinary and Adverse Actions* for reckless behaviors, including:
  - i. Reckless disregard of the procedural risks associated with non-compliance.
  - ii. Reckless disregard toward harm to self or others.
  - iii. When remedial action (e.g., education, coaching) is not



effective in changing behavior.

- g. Reckless behavior may be grounds for disciplinary action, and civil or criminal charges may be filed against the individual.

H. Just Culture Assistance:

- i. To further assist in the appropriate evaluation of these individual behaviors/actions, Human Resources, Just Culture Coordinator and Quality Safety Value Service leaders are available to coach managers using the NCPS Just Culture Decision Support Tool (JCDST). Please contact the Just Culture Coordinator at ext. 24593 for use of the NCPS Just Culture Decision Support Tool.

5. **RESPONSIBILITY:**

- A. **Medical Center Director (MCD)** – shall ensure all policies are enforced and followed, all staff is educated and trained on Just Culture. As the steward of the system, MCD is to set the prevailing Just Culture atmosphere by creating and sustaining an environment of psychological safety, fairness and partnership; promoting leadership rounds to build transparency and communicate trust. Ensuring organization systems are created and in place, showing support and an inclusive mindset of accountability and the characteristics of a High Reliability Organization from the executive level throughout the organization.
- B. **Chief of Staff (COS)** – shall present transparent focus and follow through with Just Culture structure. Ensure clinical staff is well informed and educated on Just Culture principles and trained on the JPSR reporting system. Enhance the reliability for leadership to be held accountable for psychological safety, non-punitive/non-retaliatory actions and policies are being enforced. Continue to enhance the Just Culture values through trust and transparency; and promote safety forum from executive level.
- C. **Associate Director Patient Care Services (ADPCS)** – shall make sure clinical nursing staff is educated on Just Culture; promotes psychological safety, and high reliability. Ensure nursing leadership is held accountable for actions, promoting non-punitive, non-retaliation actions and/or language is used. Create an atmosphere of teamwork, trust and transparency for all staff. Encourage staff to meet patient safety goals.
- D. **Managers** – are to be educated and shall continuously educate staff on Just Culture and support psychological safety. Provide necessary tools to staff to ensure well informed and up to date information is available. Uphold patient safety goals and guidelines. Encourage staff by rewarding staff to report, to speak up, and Stop the Line. Support staff

in the safety forum.

- E. **Staff** – shall speak up, identify errors, close calls, and report any patient safety concern. Stay informed and educated on Just Culture and psychological safety. Utilized team approach in identifying and reporting solutions to enhance patient safety. Participate in safety forums, become patient safety champions.

The interpretation, administration and monitoring of compliance with this policy shall be the responsibility of Executive Leadership and Service Chiefs in conjunction with Human Resources Management Service and Quality, Safety and Value Service.

## 6. **REFERENCES:**

NCPS Just Culture Decision Support Tool, NCPS 2019.

Connor M., et al.: Creating a fair and just culture: One institution's path toward organizational change. The Joint Commission Journal on Quality and Patient Safety 33:10, 617-624, October 2007.

Dana-Farber Cancer Institute, Principles of a Fair and Just Culture.; Frankel A., et al.: Improving patient safety across a large integrated health care delivery system. Int Journal of Qual Health Care 15 (suppl. 1):i31-i40, Dec. 2003.

High-Reliability Health Care: Getting There from Here. Chassin, Mark R., and Loeb, Jerod, The Joint Commission.org, 2013

Institute of Medicine: To Err is Human: Building a Safer Health System. Washington, DC: National Academy Press, 2000.

Just culture training for healthcare managers. The Just Culture Community. 10 June, 2008. Available at <http://www.justculture.org>.

Marx D.: Patient Safety and the "Just Culture": A Primer for Health Care Executives New York City: Columbia University, 2001.

MEDVAMC Memorandum 05-002 Disciplinary and Adverse Actions National Center for Ethics in Health Care. Ethics.va.gov

Teamwork as an Essential Component of High-Reliability Organizations  
<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1955345>

Weick, K.E. & Sutcliffe, K.M. (2007). Managing the Unexpected. 2<sup>nd</sup> ed. San Francisco: Jossey-Bass.

7. **RESCISSION:**  
None

LINDSEY J Crain  
167023

Digitally signed by LINDSEY J  
Crain 167023  
Date: 2020.02.26 15:18:48 -06'00'

FRANCISCO VAZQUEZ, MBA  
Medical Center Director

Attachments:

Attachment A – Understand a Just Culture

Attachment B - Guideline for Analyzing and Responding to a Safety Event

1.2: Just Culture Decision Support Tool (DST)

What Is the Just Culture DST?

The DST is a leadership tool that guides leaders, managers and supervisors through the process of determining the appropriate organizational response when managing employees in the wake of an adverse event or close call. The DST, Figure A3, below:

- Explains when consoling and/or coaching an employee is suitable versus where progressive discipline may be more appropriate.
- Assists in outlining the degree of organizational versus individual accountability for a given situation.
- Differentiates between human error, at-risk behavior, reckless behavior, malicious behavior and impaired behavior. A just and fair response is described for each behavior type.

Why Is This Important?

Using the DST helps your organization establish a consistent and fair administrative response with employees when failures occur. The DST avoids a rapid punitive action by forcing leaders, managers and supervisors to ask specific questions consistent with the Just Culture construct. Accepting the premise that an HRO cannot exist without trust between leaders and those working in the operational environment day to day, the key point to remember about the DST is that its consistent use builds trust between leaders and staff members over time.

Figure A3: The Just Culture Decision Support Tool (DST)

**STEP 1: Choose the column that best describes the employee's action. Read down the column for recommended responses.**

The employee was impaired by illegal or legal substances.	The employee wanted to cause harm.	The employee makes or participates in an error while working appropriately and in the patient's best interest.	The employee made a potentially unsafe choice. Faulty or self-serving decision making may be evident, or short cuts, or routine rule violations.	The employee knowingly violated a rule and / or made a dangerous or unsafe choice. The decision appears to have been made with little or no concern about risk.
<b>IMPAIRED JUDGEMENT</b>	<b>MALICIOUS ACTION</b>	<b>HUMAN ERROR</b>	<b>AT RISK Behavior</b>	<b>RECKLESS Behavior</b>
<ul style="list-style-type: none"> <li>• Discipline is warranted if illegal substances were used.</li> <li>• The employee's performance should be evaluated to determine if a temporary work suspension is helpful.</li> <li>• Help should be actively offered to the caregiver.</li> </ul>	<ul style="list-style-type: none"> <li>• Discipline and/or legal proceedings are warranted.</li> <li>• The employee's duties should be suspended immediately.</li> </ul>	<ul style="list-style-type: none"> <li>• The employee is not accountable.</li> <li>• The employee should be consoled.</li> <li>• The employee should be interviewed and consulted during any systems level analysis.</li> </ul>	<ul style="list-style-type: none"> <li>• The employee is accountable and should receive coaching.</li> <li>• The employee should participate in teaching others the lessons learned.</li> </ul>	<ul style="list-style-type: none"> <li>• Discipline may be warranted.</li> <li>• The employee is accountable and should receive re-training/coaching as necessary.</li> <li>• The employee should participate in teaching others the lessons learned.</li> </ul>

**STEP 2: If 3 other employees with similar skills and knowledge would do the same thing in similar circumstances. If YES proceed below.**

The system and/or culture supports error and requires improvement and/or re-design. Leaders are accountable and should apply error management in the system via human factors-based improvements.	The system and/or culture supports risky action and requires improvement and/or redesign. The employee is probably less accountable for the behavior. Leaders share accountability with the employee.	The system and/or culture supports reckless action and requires improvement and/or redesign. The employee is probably less accountable for the behavior. Leaders share accountability with the employee.
---	---	--

**STEP 3: If history of repeated mistakes, the employee may be in the wrong position. Evaluation is warranted and coaching, transfer or termination should be considered. The corrective action should be modified accordingly.**



Adapted from: Leonard, M.W., Frankel, A., The path to safe and reliable healthcare. Patient Educ Couns 2010 Sep;50(3):289-292.

Just Culture Decision Support Tool: Modified by NCPS in 2019. Source: Allan S. Frankel, Michael W. Leonard, and Charles R. Denham. Fair and Just Culture, Team Behavior, and Leadership Engagement: The Tools to Achieve High Reliability. HSR: Health Services Research 41:4, Part II (August 2006).

Just Culture Guide

Section 1: Understand a Just Culture *Continued*

How to Use the DST:

Step 1: Choose the column that best describes the employee's action. Read down the column for recommended responses.

As you look through the gray columns, move from left to right. Ask yourself which of the statements / definitions most accurately describes the employee's behavior. This assumes that you have talked with the employee to better understand their choices - and why they made the decisions they made as the event unfolded.

**STEP 1: Choose the column that best describes the employee's action. Read down the column for recommended responses.**

The employee was impaired by illegal or legal substances.	The employee wanted to cause harm.	The employee makes or participates in an error while working appropriately and in the patient's best interest.	The employee made a potentially unsafe choice. Faulty or self-serving decision making may be evident, or short cuts, or routine rule violations.	The employee knowingly violated a rule and / or made a dangerous or unsafe choice. The decision appears to have been made with little or no concern about risk.
<b>IMPAIRED JUDGEMENT</b>	<b>MALICIOUS ACTION</b>	<b>HUMAN ERROR</b>	<b>AT RISK Behavior</b>	<b>RECKLESS Behavior</b>

Once you determine the employee's behavior best described in the gray row, move down the corresponding column for guidance.

**STEP 1: Choose the column that best describes the employee's action. Read down the column for recommended responses.**

The employee was impaired by illegal or legal substances.	The employee wanted to cause harm.	The employee makes or participates in an error while working appropriately and in the patient's best interest.	The employee made a potentially unsafe choice. Faulty or self-serving decision making may be evident, or short cuts, or routine rule violations.	The employee knowingly violated a rule and / or made a dangerous or unsafe choice. The decision appears to have been made with little or no concern about risk.
<b>IMPAIRED JUDGEMENT</b>	<b>MALICIOUS ACTION</b>	<b>HUMAN ERROR</b>	<b>AT RISK Behavior</b>	<b>RECKLESS Behavior</b>
<ul style="list-style-type: none"> <li>Discipline is warranted if illegal substances were used.</li> <li>The employee's performance should be evaluated to determine if a temporary work suspension is helpful.</li> <li>Help should be actively offered to the caregiver.</li> </ul>	<ul style="list-style-type: none"> <li>Discipline and/or legal proceedings are warranted.</li> <li>The employee's duties should be suspended immediately.</li> </ul>	<ul style="list-style-type: none"> <li>The employee is not accountable.</li> <li>The employee should be consoled.</li> <li>The employee should be interviewed and consulted during any systems level analysis.</li> </ul>	<ul style="list-style-type: none"> <li>The employee is accountable and should receive coaching.</li> <li>The employee should participate in teaching others the lessons learned.</li> </ul>	<ul style="list-style-type: none"> <li>Discipline may be warranted.</li> <li>The employee is accountable and should receive re-training/coaching as necessary.</li> <li>The employee should participate in teaching others the lessons learned.</li> </ul>

For example, if you determine that the employee's behavior is best described by the definition for Human Error, then the guidance is:

- The employee is not accountable
- The employee *should be consoled*
- The employee *should be interviewed and consulted* during any systems level analysis

As you look at the definition for At Risk Behavior, note that the employee chooses the behavior, and that the decision is "potentially unsafe" and may depict simple rule violations seen in the everyday environment to accomplish work in the midst of production pressures (or some competing goal). This represents drift discussed in Section 1. Note that the description of Reckless Behavior again involves choices and rule violations, but the magnitude of the risk and the level of regard for that risk are differentiating factors.

### How to console staff members after human error

- Recognize the distinction between medical errors and adverse events, as staff members and clinicians can become second-victims with either.
- The second-victim is often concerned about whether the patient and family are okay after the event and about how the event might impact their career or job. Many second-victims worry about how their peers will view them after the event, whether their colleagues will trust them to deliver safe care to patients, and if the organization is going to react negatively to the event.
- Comfort your employee by leading an empathetic and/or sympathetic discussion and showing genuine concern and respect for their welfare.
- In cases where patients have been harmed, resources to care for your employee who may be a second-victim can be found at [Care for the Caregiver](#).

### How to coach staff members after at-risk behavior or drift

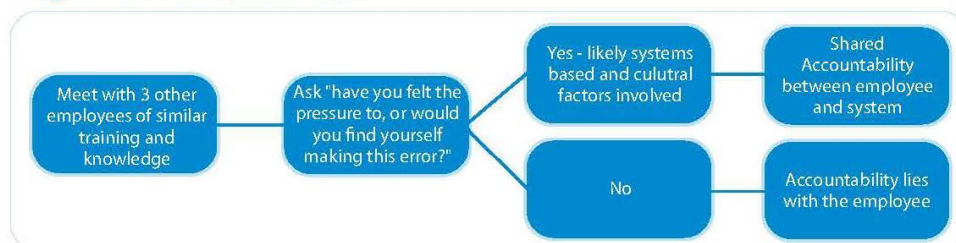
- Raise awareness and/or understanding of the risks associated with the behavior.
- Recognize that your own success is connected to the success of your employee.
- Establish an understanding of the consequences of their choices.
- Emphasize and incentivize “safety behaviors” and de-emphasize “risky behaviors.”
- Help your employee be involved in their own teaching because they are more likely to act on that teaching and apply it again to other situations.
- Ask your employee to share the actions they will take or the goals they plan to reach. Without action, the dialogue is just a conversation, not coaching.

### Step 2: Ask whether three other employees with similar skills and knowledge would do the same thing in similar circumstances. If “Yes,” proceed below.


This step, also called the *substitution test*, is mainly centered on the accountability question. We are trying to determine if the actions of the employee in question are unique – a “one off” – versus behavior that is relatively common and predictably reproduced by peers with similar training and knowledge.

For example, in **Figure A4**, take the case of a facility engineer who takes a short cut and deviates from policy and procedure to conduct preventative maintenance on medical equipment. The deviation leads to total loss of the equipment and downtime for certain diagnostic imaging services. Assume that in Step 1 we identified the engineer’s behavior as “At Risk Behavior” requiring coaching. Follow the substitution test below to determine the type of accountability.

**Figure A4: The Substitution Test**



We now ask three other engineers from the same department if they have felt pressure to or would take the same shortcut as the engineer involved in the mishap. If the answer is "yes," then there are potential systems based and cultural factors driving the behavior (such as supervisor pressure and negative behavior, or chronic short-staffed departments). In this case, we as leaders would explain to the engineer that he is accountable for the decisions he made; however, there are systems and cultural issues that factor in as well and system redesign is warranted. Accountability is therefore shared among the employee and leadership, as leaders are the stewards of the system and set the prevailing culture. This is an important discussion for leaders to have with the employee as it serves to create a sense of fairness and partnership.



**STEP 2:** If 3 other employees with similar skills and knowledge would do the same thing in similar circumstances. If YES proceed below.

<p>The system and/or culture supports error and requires improvement and/or re-design. Leaders are accountable and should apply error management in the system via human factors-based improvements.</p>	<p>The system and/or culture supports risky action and requires improvement and/or redesign. The employee is probably less accountable for the behavior. Leaders share accountability with the employee.</p>	<p>The system and/or culture supports reckless action and requires improvement and/or redesign. The employee is probably less accountable for the behavior. Leaders share accountability with the employee.</p>
--	--	---

**STEP 3:** If history of repeated mistakes, the employee may be in the wrong position. Evaluation is warranted and coaching, transfer or termination should be considered. The corrective action should be modified accordingly.

Let us suppose that when we talk to other engineers in the department that we can find no one who indicates, even remotely, that they would do the same thing as the engineer in question. There are no statements about understaffing or production pressures from the supervisor. In this case, the accountability for this At Risk Behavior lies completely with the employee.

### A Few Things to Consider

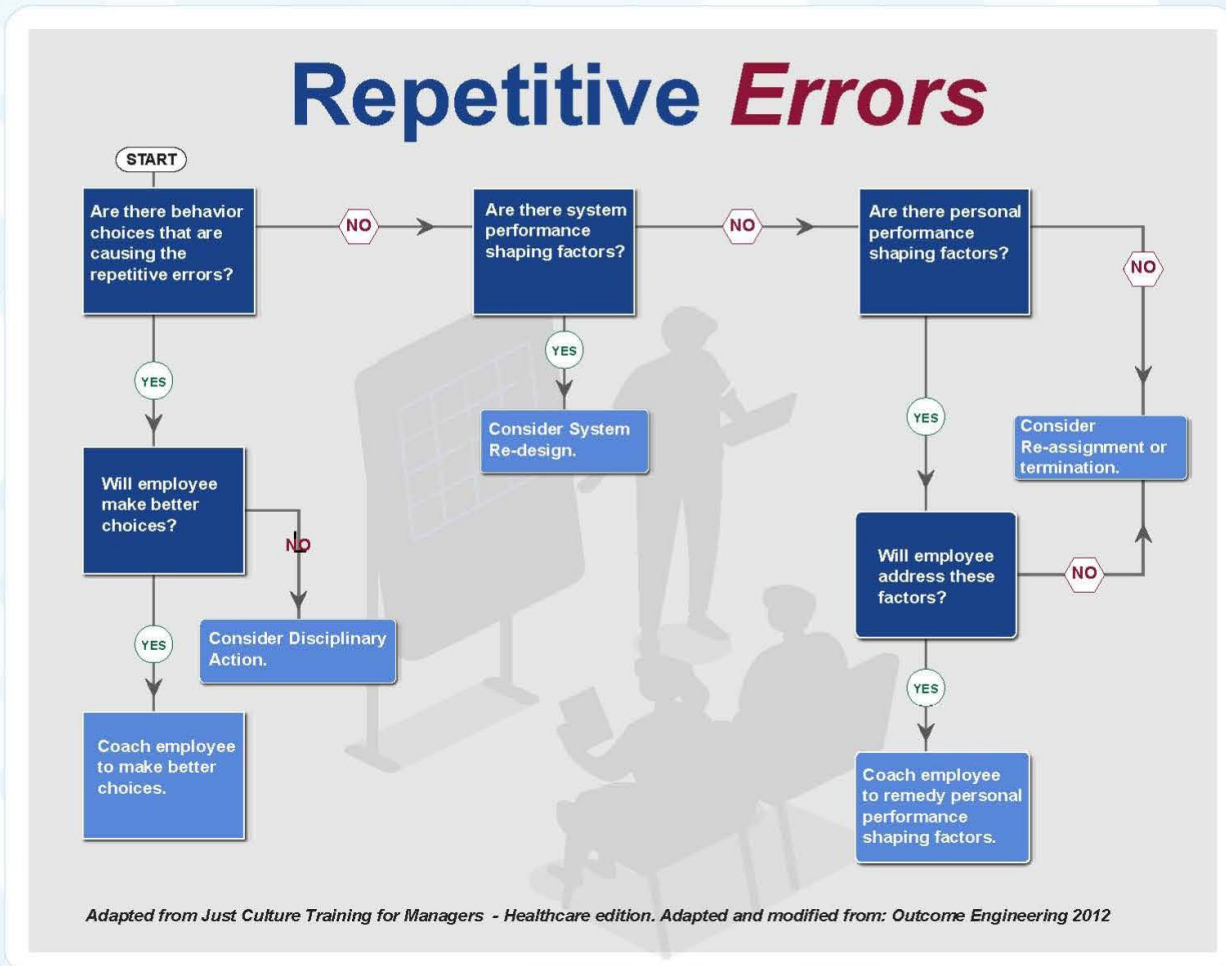
- The substitution test requires time and energy. Leaders must take the time to understand the decisions the employee made as well as locate and talk to employees with similar skills and knowledge.
- The DST suggests finding three employees for the substitution test, though it is not a hard and fast amount. The idea is to get a sense of the existing culture along with common behaviors and practices in the work area or team.
- The approved method for investigating and abating systems issues in the VHA is the RCA. This is a process that falls under the purview of Patient Safety, is protected by statute from disclosure and use for disciplinary purposes, is not concerned with questions of accountability, and occurs separately from use of the DST.
- The DST is a tool that is not protected from disclosure, does address questions of accountability, and is used by administration not Patient Safety.

**Step 3:** If there is a history of repeated mistakes, the employee may be in the wrong position. Evaluation is warranted, and coaching, transfer or termination should be considered. The corrective action should be modified accordingly (See Figure A5).

While coaching is not discipline, employees are expected to modify their behavior and choices. If there are repeated episodes of **At Risk Behavior\***, then the situation needs to be managed differently. The same applies to situations that are determined to be **Human Error**. Repeating patterns of failure require that additional questions are posed. The Repetitive Errors Algorithm on the flip side of the DST provides guidance to manage these situations.

\*The Just Culture DST should not be submitted into evidence for a HR disciplinary action. Contact your HR specialist when considering a disciplinary action to ensure the process and evidence needed.

Figure A5: Flowchart for Repetitive Errors





**Guideline for Analyzing and Responding to a Safety Event**

Behaviors/Actions Classification	Human Error	At-Risk Behavior	Reckless Behavior
Definition	Inadvertent action: Lapse, mistake	A choice: risk not recognized or believed justified	Conscious disregard of unreasonable risk (Note: Repetitive at-risk behaviors may become reckless, but manager must rule out system's contribution to the repetitive behaviors}
Manage through:	Changes in: " Processes • Procedures • Training • Design • Environment	<ul style="list-style-type: none"> <li>• Remove incentives for at-risk behavior</li> <li>• Create incentives for healthy behaviors</li> <li>• Increase awareness of risks involved (situational awareness}</li> </ul>	Follow Corrective Action Program Policy
<b>'NOTE: OUTCOMES DO NOT PREDICATE HOW WE MANAGE B EHAVIORS</b>			
Response	<p>Console the person who committed human error. These errors should be seen as a product of the system in which the employee works. The systems are what have to be corrected.</p> <p>Managers, supported by leadership should identify and change error-prone processes, procedures and environments (since managers are responsible for the environment in which the employees work.)</p>	<p>Coach non-punitively</p> <p>Identify, manage and coach at-risk behaviors proactively.</p>	<p>Corrective Action</p> <p>Follow policy</p>
Examples of Actions/Behaviors	<p>Physician orders 100mg of drug instead of 10mg.</p> <p>RN is constantly interrupted during medication administration to attend to patients needs.</p> <p>New RN programs pump incorrectly because of inadequate orientation to pump and lack of availability of preceptor.</p> <p>A patient transporter misinterprets a location code and delivers a patient to OR instead of Interventional Radiology</p>	<p>RN labels blood specimen at nursing station rather than at bedside because she has never heard of or been involved in a mislabeling incident.</p> <p>Technician does not check 2 patient identifiers and labels x-rays with wrong name.</p> <p>A housekeeper brings bleach from home and places it in her mop water in hopes of providing better cleaning and a fresher smell. She is assigned to clean up a spill of formaldehyde which has an adverse chemical reaction to the bleach in her mop water.</p>	<p>Professional provides patient care while intoxicated.</p> <p>Prior to administering blood, RN falsifies a second RN signature in violation of requirements for double check prior to blood transfusion.</p> <p>Physician has been reminded repeatedly regarding personal safe practices regarding hand washing but does not wash hands prior to examining patient.</p> <p>An office employee passes sensitive patient information about a celebrity to the local newspaper, in strict violation of hospital policy.</p>

MICHAEL E. DEBAKEY VETERANS AFFAIRS MEDICAL CENTER  
Houston, Texas

MEDICAL CENTER POLICY  
MEMORANDUM NO. 05-002

August 20, 2018

DISCIPLINARY AND ADVERSE ACTIONS

I. PURPOSE

A. The purpose of this policy is to describe the procedures for taking disciplinary or adverse action based on employee performance and/or misconduct.

B. Applicability. All Title 5, Hybrid Title 38, and Title 38 personnel are covered by this policy.

C. The public interest requires the maintenance of high standards of employee performance, integrity, conduct, and effectiveness. When such standards are not met, it is essential that prompt and just corrective action be taken. The policy of the VA is to maintain conformance with standards of conduct and performance which will promote the best interests of the VA. Where a disciplinary or adverse action is required because of non-conformance with these standards, the employee will not be penalized out of proportion to the character of his/her offense. Disciplinary and adverse actions shall be governed by these basic principles:

1. An employee will be informed honestly and specifically why the action is being taken against him or her.
2. An employee shall be given a fair chance to present his/her side of the case.
3. When replying to a proposed disciplinary or adverse action, the employee has the right not to be represented or to choose to be represented by the American Federation of Government Employees (AFGE), an attorney, or other representative. If a Bargaining Unit Employee (BUE) chooses to be represented by an entity other than AFGE, they must inform AFGE and provide a document showing AFGE has been notified.
4. Both the employee and his/her representative will be assured freedom from restraint, interference, coercion, discrimination, or reprisal in presenting their case.
5. The principle of like penalties for like offenses will be followed with due consideration for circumstances in individual cases. When deciding an appropriate penalty, consideration will also be given to whether there exists a combination or series of offenses, a prior disciplinary history or letter of counseling, or any other aggravating or mitigating factors.
6. Disciplinary and adverse actions must not be influenced by race, age, color, religion, national origin, sex, marital status, non-disqualifying

physical handicap, or partisan political reasons except when required by law.

7. The concept of progressive discipline, designed primarily to correct and improve employee performance and conduct, rather than to punish, will be followed where there is no conflict with Public Law 115-41 (Department of Veterans Affairs Accountability and Whistleblower Protection Act of 2017). If an employee's performance and/or conduct is unacceptable, the action taken by the supervisor to correct the problem will become more severe after each instance. There are clearly situations of egregious misconduct (i.e., patient abuse, sexual harassment, excessive unauthorized absence, violence in the workplace, etc.) that do not warrant the use of progressive discipline due to the seriousness of the offense.

## II. DEFINITIONS

A. **Admonishment.** An admonishment is a written statement of censure given to an employee for a minor act of misconduct. A copy of the admonishment will remain a part of the employee's record for a minimum of 6 months and a maximum of 2 years.

B. **Adverse Action.** For Title 5 and Hybrid Title 38 employees, an adverse action includes a removal, separation for medical disqualification, suspension for more than 14 days, or reduction in grade and/or pay effected by management. For Title 38 employees, all suspensions are considered adverse actions as are removals, separation for medical disqualification, or reduction in grade and/or pay effected by management.

C. **Demotion.** A demotion is an adverse action where a reduction in grade and/or pay occurs. Not all reductions in pay are considered demotions.

D. **Disciplinary Action.** An action taken to correct misconduct or other offenses, and to enforce prescribed rules of behavior. It includes admonishments, reprimands, and suspensions of 14 days or less (excludes suspensions for Title 38 employees).

E. **Official Time.** Time granted to an employee to review the material relied on to support a proposed action, to prepare an answer, to secure affidavits, and to make an oral reply, if the employee is otherwise in a duty status.

F. **Reprimand.** A reprimand is a statement of censure given for an act of misconduct. For bargaining unit employees, a copy of the reprimand will remain a part of the employee's record for a minimum of 6 months and a maximum of 3 years. The retention period for non-bargaining employees is 2 to 3 years.

G. **Suspension.** The placement of an employee in a non-duty, non-pay status.

H. Removal. The involuntary separation of a non-probationary employee for disciplinary or non-disciplinary reasons.

I. Termination. The involuntary separation of a probationary or temporary employee. (Also called a discharge for Title 38 employees.)

### III. PROCEDURES

A. Managers and supervisors are encouraged to utilize written counselings as a means of corrective action to prevent future occurrences of minor infractions. Letters of counseling should be retained by the employee's supervisor since letters of counseling may be used at a later date to support a request for a disciplinary or adverse action.

B. In cases involving a potential disciplinary or adverse action, inquiry will be made into the incident or situation as soon as possible to obtain the facts and determine what action, if any, is warranted. This may consist of the collection of evidence and/or witness statements; a manager convened fact-finding; an Administrative Board of Investigation convened by the Medical Center Director; or referral to the Office of Inspector General. The type of inquiry or investigation conducted will be determined by the circumstances surrounding the alleged misconduct.

C. Once all evidence has been collected, the supervisor should forward the evidence and a request for appropriate action to the Labor Management Relations office. The complete evidence in support of any action is submitted by the current human resources information system (HRIS) utilized for processing personnel action requests. Currently the HRIS system available to all Service and Care lines for requesting personnel actions is WebHR.

D. The Labor Management Relations Office will review the evidence and the request to determine if disciplinary or adverse action is warranted and supported by the evidence. If warranted, the Labor Management Relations Office will prepare the appropriate documents for signature.

E. Delegated authorities to sign a proposed disciplinary/adverse action letter or a decision letter are outlined on Attachment A for Title 5 and Hybrid Title 38 employees, and Attachment B for Title 38 employees.

F. For an AFGE bargaining unit employee, Article 14, Section 10, of the 2011 Master Agreement states an employee who is the subject of an investigation will be informed of their right to union representation before they are questioned or a signed statement from that employee is obtained.

G. Terminations:

1. Temporary employees and probationary employees, Veterans Readjustment Appointment (VRA) and Term Appointment employees serving a probationary or trial period do not ordinarily receive disciplinary and/or adverse actions. If the employee commits an infraction serious enough to warrant a disciplinary or adverse action, the supervisor should consider termination. A written recommendation for the termination will be submitted to Labor Management Relations Section (05/LMR) along with supporting evidence.
2. This is the only portion of this policy that is applicable to the disciplinary or adverse action procedures regarding probationary, VRA, term, and temporary employees.

IV. RESPONSIBILITIES

A. Supervisors and managers are responsible for:

1. Ensuring allegations of employee misconduct are fully and fairly investigated. Investigation of the situation may include, but is not limited to, gathering and analyzing written statements from each possible witness; copies of timecards; copies of prior discipline, counseling, or referral; copies of police reports; and/or any other available evidence that misconduct occurred. In every case, inquiry will be made into the incident or situation as soon as possible.
2. Submitting the complete evidence file to the Labor Management Relations Office (05/LMR) of Human Resources, when investigation sustains that misconduct occurred.
3. Consulting with the Labor Management Relations Office when an employee is failing his/her performance standards.

B. The Labor Management Relations Office is responsible for:

1. Assisting managers and supervisors with disciplinary and adverse action matters, interpreting regulations and statutes, ensuring consistency, recommending sound personnel practices, reviewing existing policies and making appropriate changes.
2. Preparing disciplinary and adverse action letters to ensure compliance with VA policy, regulations, and statutes.
3. Advising and assisting employees on matters relating to their rights to appeals and hearings, and providing information and interpretation of disciplinary and adverse action procedures, regulations and statutes.

C. Employees are responsible for:

1. Conducting themselves both on and off the job in a manner reflecting favorably on them personally and on the Federal government.
2. Abiding by standards of conduct, laws, rules, regulations, policies, and procedures. Reporting any observed incidents of misconduct to the appropriate authority (i.e. supervisor, police, etc.)
3. Obtaining advice from authoritative agency officials (supervisors, Labor Management Relations Office personnel, Regional Counsel, etc.) on any unclear or questionable rules of conduct prior to engaging in the conduct.
4. Providing full and truthful answers during any inquiry or investigation. The only time employees are entitled to remain silent is if they may potentially incriminate themselves in a *criminal* offense.

V. REFERENCES

[Public Law 115-41, Department of Veterans Affairs Accountability and Whistleblower Protection Act of 2017](#)

Human Resources Management Letter (HRML)-05-17-05-Adverse Action Procedures (T5\_Hybrid Non-BUE)

Human Resources Management Letter (HRML)-05-17-06-Adverse Action Procedures (T5\_Hybrid Non-BUE and BUE)

Human Resources Management HRML-05-17-07 - Disciplinary and Major Adverse Action Procedures (T38 Non-BUE)

Human Resources Management HRML-05-17-08 - Disciplinary and Major Adverse Action Procedures (T38 Non-BUE and BUE)

[VA Directive and Handbook 5021.](#)

[VA Directive and Handbook 5025.](#)

[Master Agreement between the Department of Veterans Affairs and the American Federation of Government Employees, effective March 2011.](#)

VI. RESCISSION

Medical Center Policy Memorandum No. 05LMR-001, *Disciplinary and Adverse Actions* dated July 9, 2015.

FRANCISCO VAZQUEZ  
Medical Center Director

Attachment A: Delegated Authorities for Title 5 and Hybrid Title 38 employees

Attachment B: Delegated Authorities for Title 38 employees

**Attachment A  
Delegated Authority for  
Title 5 and Hybrid Title 38 bargaining unit employees\*:**

<b>Type of Action</b>	<b>Proposing Official</b>	<b>Deciding Official</b>
Admonishment	Immediate Supervisor**	Service or Care Line Executive or equivalent
Reprimand	Immediate Supervisor**	Service or Care Line Executive or equivalent
Suspensions of 3 calendar days or less	Immediate Supervisor or Higher	Service or Care Line Executive or equivalent
Suspensions of 4 to 14 calendar days	Immediate Supervisor or Higher	Supervising member of senior management (Medical Center Director, Deputy Director, Associate Director, Associate Director for Patient Care Services, or Chief of Staff)
Suspension over 14 calendar days, removals, demotions, or other adverse actions	Service or Care Line Executive or equivalent	Medical Center Director
Termination of temporary employees	Service or Care Line Executive or equivalent***	HR Manager
Termination of probationary employees	Service or Care Line Executive or equivalent***	HR Manager

\*Specified authorities include individuals officially designated to be in an acting capacity.

\*\*Non-bargaining employees do not receive letters of proposed admonishment or proposed reprimand.

\*\*\*Requests for Termination must be submitted to HR Manager. No proposal letter is provided to the individuals.

NOTE: These delegations do not pertain to disciplinary or adverse actions taken for employees at the Service/Care Line Executive or higher level.



**Attachment B**  
**Delegated Authority for Title 38 employees\*:**

<b>Type of Action</b>	<b>Proposing Official</b>	<b>Deciding Official</b>
Admonishment	Immediate Supervisor	Service or Care Line Executive or equivalent
Reprimand	Immediate Supervisor	Service or Care Line Executive or equivalent
All suspensions	Service or Care Line Executive or equivalent	Medical Center Director
Removals, demotions, or other adverse actions	Service or Care Line Executive or equivalent	Medical Center Director
Termination of temporary or part-time employees serving under 38 USC 7405(a)1(A)	Service or Care Line Executive or equivalent**	HR Manager
Termination of probationary employees (post-Summary Review Board)	Service or Care Line Executive or equivalent**	HR Manager

\*Specified authorities include individuals officially designated to be in an acting capacity.

\*\*Requests for Termination must be submitted to HR Manager. No proposal letter is provided to the individuals.

NOTE: These delegations do not pertain to disciplinary or adverse actions taken for employees at the Service/Care Line Executive or higher level.

MICHAEL E. DEBAKEY VETERANS AFFAIRS MEDICAL CENTER  
Houston, Texas

MEDICAL CENTER POLICY  
MEMORANDUM NO. 05-014

October 9, 2019

VA GRIEVANCE PROCEDURES

I. PURPOSE

A. The purpose of this policy is to establish MEDVAMC policy, principles and procedures for grievance presentation and consideration by all (1) non-bargaining unit employees and (2) *permanent and probationary* Title 38 bargaining unit employees only when appealing a disciplinary or adverse action which does not involve a question of professional conduct or competence.

B. It is the policy of the MEDVAMC to identify, prevent, and make reasonable efforts to resolve employee dissatisfactions. All individuals involved in the grievance process are expected to be candid and to act in good faith in their attempt to resolve dissatisfactions. Supervisors are expected to give full, fair, and prompt consideration to employee complaints and causes of dissatisfaction. Objective consideration of complaints or criticism affords a means of focusing attention on conditions which may require corrective action. It also provides a means within the organization of initiating and effecting desirable changes as well as taking preventive action.

C. No employee will take or threaten to take any act of reprisal against another employee because the employee has exercised or expressed an intention to exercise their right to file a grievance. No employee or employee representative will be restrained, coerced, interfered with, discriminated against, or in any way treated prejudicially in connection with the exercising of rights under the grievance procedures.

II. DEFINITIONS

A. Deciding Official. An official designated to (1) receive and attempt to adjust formal grievances; (2) refer formal grievances for further review and inquiry; and (3) decide formal grievances based on the results of impartial reviews and recommendations.

B. Disciplinary and Adverse Actions. Disciplinary and adverse actions include, but are not limited to, admonishments, reprimands, suspensions, demotions resulting in a loss of grade or pay, and removals. Excluded for purpose of this policy are adverse actions involving questions of professional conduct or competence.

C. Grievance. A request by an employee, or group of employees, for personal relief in a matter of concern or dissatisfaction relating to employment which is subject to the control of agency management.

Matters generally not covered by the grievance procedure may be found in Attachment A.

- D. Official Time. Time granted to an employee to present a grievance, if otherwise in a duty status, without charge to leave.
- E. Personal Relief. A specific remedy directly benefiting the grievant, but may not include a request for disciplinary action or other action affecting another employee.
- F. Reduction in Basic Pay. The involuntary reduction of the annual rate of basic pay to which an employee is entitled. This includes a reduction in the market pay of a physician or dentist as a result of an involuntary reassignment or change in assignment when taken for disciplinary reasons. It does not apply to reductions in pay other than basic pay, such as the loss of or reduction in performance pay, nurse executive special pay, head nurse differential, other differentials, allowances or premium pay such as standby, on-call, shift, overtime, Sunday, holiday, night work, hazardous pay, and interim geographic adjustment.
- G. Reduction in Grade. The involuntary assignment to a lower grade on the same pay scale.
- H. Title 5 and Hybrid Title 38 Employees. The grievance procedures outlined in this policy are available to all employees of the medical center except the following:
  - 1. A non-citizen appointed under Civil Service Rule VIII, Section 8.3 of Title 5, Code of Federal Regulations;
  - 2. An alien appointed under Section 1471(5) of Title 22, United States Code;
  - 3. An individual paid from funds as defined in section 2105(c) of Title 5 (not applicable to the VA) or section 4202(5) of title 38, United States Code (i.e., Excepted Service Veterans Canteen Service employees); and
  - 4. Bargaining unit employees covered by the provisions of Article 43 of the Master Agreement between VA and AFGE.
- I. Title 38 Employees

Title 38 employees covered by this policy include *permanent and probationary* physicians, dentists, podiatrists, chiropractors, optometrists, nurses, nurse anesthetists, physician assistants, and expended-function dental auxiliaries. A bargaining unit Title 38 employee may elect to use the VA grievance procedure described in this policy or the negotiated grievance procedure, but not both, in the case of a disciplinary or major adverse action that does not involve a question of professional conduct or competence.

### III. PROCEDURES

#### A. Representational Guidance

1. An employee may present a grievance with or without representation and has the right, if he/she so chooses, to be accompanied, represented and advised by a representative of his/her choice at any stage of the procedure.
2. If a grievance is presented under the formal grievance procedure, designation of a representative will be in writing. Any change of representative will be in writing.
3. A representative may be disallowed because of priority needs of the service/care line or service; unreasonable cost to the Government; conflict of position; or conflict of interest. The disallowance of a representative will be in writing, and will be issued by the Labor Relations office in Human Resources Service.

#### B. Informal and Formal Procedures

1. Informal Grievance Procedures. The employee or their representative must file an informal grievance within 15 calendar days from the date of the incident or action on which the grievance is based. When an employee is informed of a final decision that has not yet been effected, the period to present a grievance is counted from the date of notification of the action. Grievances must be filed with the lowest level official who can resolve the grievance. The grievance must clearly state the issue to be resolved and the personal relief requested. The initial presentation, which may be oral or written, is normally made to the immediate supervisor. A written informal grievance is highly recommended in order to prevent any misunderstanding regarding what is being grieved and what relief is being requested. (A sample for a written grievance is provided as Attachment B.) If the grievance is presented orally, the

employee must make clear that he/she is presenting a grievance, in order to distinguish grievances from mere inquiries or complaints. Supervisors who receive oral grievances will prepare a written summary of the oral presentation and will notify the grievant of their decision, in writing, within 10 calendar days from the date of the informal grievance. If the relief sought is not granted, the employee should be advised of the right to present the grievance under the formal procedure. (Grievances of disciplinary and adverse actions will be initiated at the formal step of the grievance procedure.)

2. Formal Grievance Procedures

- a. If an employee is not satisfied with the informal grievance decision or is grieving a disciplinary or adverse action, the employee may present a grievance, in writing, under the formal procedure. (A sample for a written grievance is provided as Attachment B.) The formal grievance must be filed through supervisory channels within 10 calendar days after receipt of the informal grievance decision, or 15 calendar days from the date of notification of a disciplinary or adverse action. Grievances that must first be processed at the informal step and fail to comply with this procedural requirement, will be returned to the employee.
- b. The formal grievance will be in writing, and must contain the following information:
  - (1) The specific action or incident on which the grievance is based, the date the action or incident occurred, and the date the employee first learned of the action or incident;
  - (2) The reasons for which the employee believes that the action was unjustified or that the employee was treated unfairly; and/or the specific policy, written agreement, or regulation violated and how it affected the employee; and
  - (3) The personal relief requested by the employee.
- c. If any of the above information is missing, the employee will be given an opportunity to furnish the information. If the employee fails to provide the necessary information by the deadline given, the grievance will be canceled.

- d. If the deciding official is unable to resolve the grievance in a timely manner acceptable to the employee, the grievance will be referred for inquiry by an examiner or for technical review by an appropriate official within 10 days of the decision official's receipt of the formal grievance.
- e. When a formal grievance is submitted, the Labor Relations supervisor will be notified promptly by the management official. The Labor Relations specialist responsible for the care/service line will establish a grievance file, separate from the employee's OPF.
- f. The deciding official, in conjunction with the Labor Relations office, will determine if a grievance examiner will be appointed or, whether the issue will be referred to VA Central Office if the primary issue involves only the interpretation of regulation or policy.
- g. If a grievance examiner is appointed, the appointee will contact the Labor Relations office for guidance and information on processing the grievance in accordance with the procedures outlined in VA Handbook 5021. Except in unusual cases or circumstances, a local grievance examiner's report will be furnished to the deciding official within 30 calendar days of the appointment.
- h. The deciding official will render a decision, in writing within 15 calendar days after the decision official receives the examiner's report.

#### IV. RESPONSIBILITIES

- A. Deciding officials are responsible for ensuring decisions are rendered in a timely manner.
- B. Supervisors are responsible for listening to employee complaints and attempting to clarify and make reasonable adjustments to address problems that arise in daily relationships with employees.
- C. The Labor Relations supervisor and staff are responsible for providing guidance and technical advice to management officials, supervisors, and employees regarding the administration of grievance procedure.

- D. Grievance Examiners are responsible for making an impartial and objective inquiry regarding the merits of a grievance and for providing a report of findings and recommendations to the decision official as well as the parties involved within the prescribed time limits.

V. REFERENCES

VA Directive and Handbook 5021; Employee-Management Relations.

VI. RESCISSION

Medical Center Policy Memorandum No. 05-014, *VA Grievance Procedure*, dated September 24, 2016.

*Lindsey Crain*

FRANCISCO VAZQUEZ, MBA  
Medical Center Director

Attachment A    Actions and Complaints Excluded from Coverage Under the VA  
Grievance Procedure

Attachment B    Sample VA Grievance Format

ACTIONS AND COMPLAINTS EXCLUDED  
FROM COVERAGE UNDER THE VA GRIEVANCE PROCEDURE

The following list reflects information provided in VA Handbook 5021 as of the date of publication of this local policy. Therefore, any questions concerning whether an issue can be grieved should be directed to the Labor Relations office. Following are specific issues excluded from the VA grievance procedures:

1. Title 38 adverse actions that involve a question of professional conduct or competence.
2. Disputes over whether a matter or question concerns, or arises out of, professional conduct or competence.
3. Separation during a probationary or trial period or of a temporary employee.
4. Complaints arising from failure to receive special advancement.
5. Complaints arising from failure to receive a promotion or reassignment.
6. Complaints arising from dissatisfaction with grade or pay on initial appointment.
7. Complaints arising from actions taken due to the individual's physical or mental condition.
8. Complaints arising from dissatisfaction with proficiency rating.
9. An action which terminates a temporary promotion within a maximum period of two years or at the completion of a project or specified period, or at the end of a rotational assignment, and returns the employee to the position from which the employee was temporarily promoted, or reassigns the employee to a different position that is not at a lower grade or pay than the position from which the employee was temporarily promoted.
10. The content of published VA or VHA regulations and policies.
11. A decision which is appealable to the Merit Systems Protection Board or subject to final administrative review by Office of Personnel Management (OPM), the Federal Labor Relations Authority (FLRA), or the Office of Worker's Compensation Programs (OWCP), under law or regulations, or any other matter for which final administrative authority lies outside VA.
12. Allegations of discrimination on the basis of race, color, religion, sex, national origin, age (over 40) and/or handicap, in connection with any decision or action.



13. A preliminary warning notice of an action that, if effected, would be covered under a grievance or appeal system or excluded from coverage.

14. Disapproval or non-adoption of a suggestion, disapproval of a quality step increase or a discretionary award, performance award, or disagreement with the amount of the award.

15. A matter that includes specified relief that is not personal to the grievant or is not subject to the control of management.

16. A matter covered by a negotiated grievance procedure. However, an employee may elect to use the VA grievance procedure or the negotiated grievance procedure in the case of a Title 38 disciplinary or major adverse action, which does not involve a question of professional competence or conduct.

17. A grievance of an individual from outside VA.

18. Grievances concerning the number of positions to be filled, or the grade level at which positions are advertised or filled.

19. An action taken in accordance with the terms of a formal agreement voluntarily entered into by an employee.

20. Matters that are not directly related to the employee's conditions of employment.

21. Matters involving the methods, means or technology of performing work.

22. Determinations and authorizations, including those delegated by the Secretary, regarding the approval, disapproval, or amount of market or performance pay and pay granted to a nurse executive.

23. Designations of employees to serve on a Disciplinary Appeals Boards are selected, designations of employees to serve on Disciplinary Appeal Boards, professional standards boards, compensation panels, or the appointment of a grievance examiner.

24. All matters for which review procedures are already established in VA policy.

25. A decision not to remove an admonishment or reprimand from an employee's OPF prior to the expiration date.

26. Non-selection for promotion from a group of properly ranked and certified candidates or failure to receive a non-competitive promotion.

27. Grievances regarding SES employees (with limited exceptions).
28. An action which terminates a temporary promotion.
29. The content of the critical elements and performance standards.
30. Return of any employee from an initial appointment as a supervisor or manager to a nonsupervisory or non-managerial position for failure to satisfactorily complete the probationary period.
31. Separation of employees with less than 1 year of current continuous employment appointed under authority of Schedule A or Schedule B.

SAMPLE VA GRIEVANCE FORMAT

DATE:

To: (Name, title, and mailing symbol)

SUBJ: Grievance

FROM:

1. This is a (formal or informal) grievance under the VA grievance procedures.
2. The matter on which this grievance is based occurred in (give date) and is described in detail as follows: (furnish sufficient detail to clearly identify the matter being grieved. Appropriate documents related to your grievance should be attached.
3. The personal relief (i.e., corrective action) I seek is: (specify clearly.)

Signature  
Name and Title

Attachments: (all attachments should be identified)

**EMPLOYEE CODE OF CONDUCT, CUSTOMER SERVICE STANDARDS OF  
BEHAVIOR, AND MANAGEMENT OF DISCOURTEOUS, DISRUPTIVE, AND/OR  
BULLYING BEHAVIOR**

**MCP 05-024**

Michael E. DeBakey Veteran Affairs  
Medical Center  
Houston, TX 77030

**Rescinded Document:**  
See paragraph 7.

**Signatory Authority:**  
Francisco Vazquez, MBA  
Medical Center Director

**Effective Date:**  
July 18, 2022

**Recertification Date:**  
July 18, 2027

**Responsible Owner:**  
Chief, Strategic Business Unit

## **1. POLICY**

This medical center policy serves to inform all employees that discourteous, disruptive, and/or bullying behavior is subject to corrective action up to and including removal from the workforce and may also be subject to criminal prosecution.

## **2. JUSTIFICATION**

The purpose of this policy memorandum is to outline expected standards of behavior for members of the Michael E. DeBakey VA Medical Center (MEDVAMC) workforce necessary to maintain an environment promoting customer satisfaction and patient centered care principles as well as ensuring a workplace free of discourteous, disruptive, and/or bullying employee behavior.

The provisions of this memorandum apply to all employees and others working for or at the Michael E. DeBakey VAMC, whether in the Medical Center proper or in an off-site location. These employees and others include all full-time, parttime and intermittent Title 5, Title 38 and Hybrid Title 38 employees, station fee basis and/or contract employees, consultants, volunteers, without compensation (WOC) employees, students, residents, and individuals appointed under the Intergovernmental Personnel Act working for, or at, the MEDVAMC This policy exists due to an absence of national policy or guidance.

## **3. RESPONSIBILITIES**

a. **VA Medical Facility Director.** The VA medical facility Director is responsible for:

1. Ensuring a safe, comfortable, and productive workplace for all MEDVAMC staff, patients, and visitors.
2. Fostering an environment that allows every member of our healthcare team, patients, and visitors to feel free to safely voice their opinions and/or concerns,

including the removal of fear commonly associated with identifying concerns or disagreeing with those in positions of authority.

3. Ensuring the overall effectiveness of this policy.

b. **Chief, Human Resources Management.** The Chief, Human Resources Management is responsible for:

1. Providing guidance to managers and supervisors on addressing concerns related to employee discourteous, disruptive and/or bullying behavior in the workplace.
2. Ensuring that corrective action(s) taken towards an employee follow the policies and procedures established in VA policies and Labor Union Contracts.

c. **Medical center managers and supervisors.** Medical center managers and supervisors are responsible for:

1. Ensuring a safe, comfortable, and productive workplace for all MEDVAMC staff under their supervision.
2. Fostering an environment that allows every member of our healthcare team, patients, and visitors to feel free to safely voice their opinions and/or concerns, including the removal of fear commonly associated with identifying concerns or disagreeing with those in positions of authority.
3. Recognizing employee behaviors that represent exemplary service and demonstration of the organization's core values and characteristics.
4. Holding employees accountable for behaviors that are contrary to the requirements of this policy including: a. Discourteous, disruptive, and/or bullying behavior against other employees, patients or visitors, or b. Failure to report information concerning employee discourteous, disruptive, and/or bullying behavior, or c. Engagement in any form of retaliation against an employee, patient or visitor who has reported employee discourteous, disruptive, and/or bullying behavior through appropriate channels.
5. Ensuring that employees under their supervision and patients and visitors to their area receive prompt and appropriate medical attention in the event of an injury resulting from discourteous, disruptive, and/or bullying behavior in the workplace and that the appropriate personnel are notified of a work-related injury.
6. Ensuring that employees who have been verbally or physically assaulted, have witnessed violent behavior in the workplace, or have exhibited signs of psychological distress associated with potential violent behavior are offered the Employee Assistance Program (EAP).
7. Ensuring "Customer Service" is a critical element in all employees' performance standards.

8. Ensuring that all job candidate interviews contain a customer service component and that customer service skills, including communication, are a key component in the selection decision.
- d. **Education Service Line Executive.** The Education Service Line Executive is responsible for providing training to MEDVAMC staff on the provisions of this policy.
  - e. **VA Chief of Police.** The VA Chief of Police is responsible for responding to and investigating incidents of employee discourteous, disruptive and/or bullying behavior that involve actual physical violence or a threat of physical violence, or when deemed appropriate.
  - f. **Employees, volunteers, and other staff.** Employees, volunteers, and other staff are responsible for:
    1. Following safe work practices and fostering an environment that allows every member of the healthcare team, patients, and visitors to feel free to safely voice their opinions and/or concerns to include the removal of fear commonly associated with identifying concerns or disagreeing with those in positions of authority.
    2. Completing assigned customer service, code of conduct, and education and awareness training on harassment prevention.
    3. Reporting employee discourteous, disruptive, and/or bullying behavior to their supervisor and/or the VA Police and/or the Employee Threat Assessment Team (ETAT), or the Harassment Prevention Coordinator.

#### 4. OTHER PARAGRAPHS

##### a. Basic principles:

It is the policy of the MEDVAMC every employee should strive to make encounters with others an experience in which others are listened to carefully and treated respectfully. Attachment A provides the medical center's core values and characteristics that should be demonstrated by all members of the workforce.

MEDVAMC employees at every level are empowered to build a healing environment where every interaction conveys listening, respect, and understanding.

The mistreatment or abuse of others by employees will not be tolerated Retaliation, or attempted retaliation, against anyone who reports or participates in an investigation of employee discourteous, disruptive, and/or bullying behavior will not be tolerated.

**b.** Discourteous, disruptive, and/or bullying behavior includes any behavior that undermines the effectiveness of the healthcare team, which can compromise the mission and integrity of our healthcare system. Such behavior can be verbal and/or

physical and has the impact of intimidating, demeaning, frightening, and/or physically harming another employee, patient, or visitor. Attachment B provides a list of common behaviors considered discourteous, disruptive, and/or bullying in nature. Attachment C provides examples of personal conduct to minimize discourteous, disruptive, and/or bullying behavior. The main categories of discourteous, disruptive, and/or bullying behavior include:

**1.** Physical Aggression is unwanted physical contact or attempt to inflict physical harm to another individual.

**2.** Property Aggression is behavior that causes damage or destruction to private or government property.

**3.** Verbal Aggression is spoken interaction that may serve as a warning sign of physical aggression.

**4.** Passive Aggression is behavior where aggression is expressed in non-active ways such as stubbornness, sullenness, procrastination, or intentional inefficiency.

**c.** Threatening behavior includes the expression of present, conditional, or future intent to cause physical or psychological harm.

**d.** An expression constitutes a threat regardless of whether the party communicating it has the present ability/means to do harm and regardless of whether the expression is current, conditional, or future.

**e.** Bullying involves the repeated and intentional use of force, threat, or coercion to abuse, intimidate, or aggressively dominate another person. Bullying behaviors include non-verbal intimidation (stares/glances), physical threats, yelling or humiliating someone in front of others, and the spreading of information that is the topic of gossip or rumors. In contrast to conflict, bullying involves the perception by the bully, or other person, that there is an imbalance of social or physical power.

**f.** The Four-Way Test is a self-test to help you decide if a certain behavior is acceptable or appropriate. Of each thing we think, say, or do:

**1.** Is it the TRUTH?

**2.** Is it FAIR?

**3.** Will it build GOODWILL and BETTER RELATIONSHIPS? Will it BENEFIT OTHERS?

**4.** The Employee Threat Assessment Team (ETAT) is a facility-level, interdisciplinary team whose primary charge is using evidence-based and data-driven

practices for addressing the risk of violence posed by employee-generated behavior(s) that are disruptive or that undermine a culture of safety.

**g. PROCEDURES**

1. This policy memorandum will be reviewed with all employees during New Employee Orientation.
2. Any employee discourteous, disruptive, and/or bullying behavior in the workplace that constitutes actual physical aggression or a perceived threat to personal safety must be reported immediately to the VA Police (ext. 27106 or 911 in emergency situations). The Chief of Police or designee will investigate the incident, notify the Medical Center Director, and determine if a criminal violation has been committed.
3. For any incident of employee-initiated discourteous, disruptive, and/or bullying behavior in the workplace that does not constitute physical violence or threat of bodily harm, the manager(s) who receive the complaint must initiate and conduct a timely inquiry. This inquiry involves notifying Labor Relations and determining first whether immediate action is necessary, such as physical separation of employees or placing one or more employee in an off-duty status. The findings from the inquiry must determine whether corrective action is warranted.
4. At any time during the inquiry phase, a manager conducting an inquiry may seek guidance from Human Resources or the ETAT as to a recommended course of action. Common courses of action include mediation, referral to the Employee Assistance Program, and/or disciplinary action.

**5. DEFINITIONS**

None

**6. REFERENCES**

- a. Public Law 91-596; Executive Order 12196; MP-3, Part III.
- b. VA Handbook 0730, "Security and Law Enforcement"
- c. VA Handbook 5021, "Employee/Management Relations"
- d. Medical Center Policy Memorandum 00-004, "Employee Threat Assessment Team"
- e. Medical Center Policy Memorandum 05-007, "Employee Assistance Program"

**RESCISSION**

**7. RESCISSION**



Medical Center Policy Memorandum No. 00-002, Employee Code of Conduct and Management of Discourteous, Disruptive and Bulling Behavior, dated July 21, 2015.

Medical Center Policy Memorandum No. 05-016, Customer Service Standards of Behavior, dated July 11, 2018

## 8. REVIEW

MCP will be reviewed prior to the recertification date outlined below or when any changes to national policy, U.S.C., VA Directives, and/or VA Handbooks require a review to ensure compliance.

## 9. RECERTIFICATION

This MCP is scheduled for recertification on or before the last working day the month of expiration. This MCP will continue to serve as local policy until it is recertified or rescinded. In the event of contradiction with national policy, the national policy supersedes and controls.

## 10. SIGNATORY AUTHORITY

*Lindsey Crain*

Francisco Vazquez, MBA  
Michael E. DeBakey VA Medical Center Director

**Date Approved:**

**NOTE:** *The signature remains valid until rescinded by an appropriate administrative action.*

**DISTRIBUTION:** MEDVAMC SharePoint site.

**Integrity** - Act with high moral principle. Adhere to the highest professional standards. Maintain the trust and confidence of all with whom I engage.

**Commitment** - Work diligently to serve Veterans and other beneficiaries. Be driven by an earnest belief in VA's mission. Fulfill my individual responsibilities and organizational responsibilities.

**Advocacy** - Be truly Veteran-centric by identifying, fully considering, and appropriately advancing the interests of Veterans and other beneficiaries.

**Respect** - Treat all those I serve and with whom I work with dignity and respect. Show respect to earn it.

**Excellence** - Strive for the highest quality and continuous improvement. Be thoughtful and decisive in leadership, accountable for my actions, willing to admit mistakes, and rigorous in correcting them.

### **Core Characteristics**

**Trustworthy** – VA earns the trust of those it serves--every day--through the actions of all employees. They provide care, benefits, and services with compassion, dependability, effectiveness, and transparency.

**Accessible** – VA engages and welcomes Veterans and other beneficiaries, facilitating their use of the entire array of its services. Each interaction will be positive and productive.

**Quality** – VA provides the highest standard of care and services to Veterans and beneficiaries while managing the cost of its programs and being efficient stewards of all resources entrusted to it by the American people. VA is a model of unrivalled excellence due to employees who are empowered, trusted by their leaders, and respected for their competence and dedication.

**Innovative** – VA prizes curiosity and initiative, encourages creative contributions from all employees, seeks continuous improvement, and adapts to remain at the forefront in knowledge, proficiency, and capability to deliver the highest standard of care and services to all of the people it serves.

**Agile** – VA anticipates and adapts quickly to current challenges and new requirements by continuously assessing the environment in which it operates and devising solutions to better serve Veterans, other beneficiaries, and Service members.

**Integrated** – VA links care and services across the Department; other federal, state, and local agencies; partners; and Veterans Service Organizations to provide useful and understandable programs to Veterans and other beneficiaries. VA's relationship with the Department of Defense is unique, and VA will nurture it for the benefit of Veterans and Service members.

\*This list is not intended to cover all possible forms of discourteous/disruptive behavior, the intent is to list those commonly encountered in the workplace.

1. Fighting, threatening, attempting to inflict bodily harm, or dangerous horseplay.
2. Inappropriate physical contact (kissing, hugging, patting, stroking, hand touches).
3. Invasion of physical space in a threatening manner, even without contact.
4. Throwing objects, hitting, pushing, shooting, stabbing.
5. Tampering with, or causing damage, destruction, or loss to, private or government property (vandalism, theft, intentional waste).
6. Yelling.
7. Posting of inappropriate photos (nudity, sexual innuendos, demeaning images).
8. Sexual comments and/or innuendos (gestures, facial expressions, inappropriate gifts).
9. Profane, obscene, abusive, or disrespectful language.
10. Participation in rumors and/or gossip that seek to demean or discredit an employee's reputation.
11. Offensive, embarrassing, or insulting written or verbal comments about another individual.
12. Name-calling.
13. Outbursts of anger.
14. Speaking negatively about our medical center in any manner to patients, visitors, staff, etc., while on duty.
15. Inappropriate jokes (racial, ethnic, sexual, religious, age, disability).
16. Condescending language or tone of voice.
17. Challenging or daring an individual.
18. Criticizing others in front of patients, visitors, or staff.
19. Dishonesty, lying, or attempting to deceive.
20. Deliberate failure to adhere to organizational policies or procedures.
21. Exhibiting uncooperative attitudes during routine activities.
22. Reluctance or refusal to answer questions, return phone calls or pages, or respond to electronic mail.
23. Ignoring the needs of others by purposefully not following through.
24. Undermining or deliberately impeding another person's work.
25. Treating someone differently because they belong to a certain group.
26. Acting in a prejudicial, discriminatory, or scapegoating manner while profiling others.
27. Causing fear in or attempting to intimidate others by bullying, hazing, or teasing.
28. Creating a hostile work environment or allowing one to persist.
29. ANY form of retaliation for reporting discourteous/disruptive behavior.

**DO:**

- ✓ Project calmness. Move and speak slowly, quietly, and confidently.
- ✓ Acknowledge the person's feelings and indicate that you can see he/she is upset.
- ✓ Be an empathetic and active listener. Encourage the person to talk and listen patiently.
- ✓ Use delaying tactics, which will give the person time to calm down.
- ✓ Be reassuring and point out options.
- ✓ Maintain a relaxed yet attentive posture and position yourself at a right angle, rather than directly in front of the other person.
- ✓ Arrange yourself so that a person cannot block your access to an exit.
- ✓ Ask for small, specific favors such as asking the person to move to a quieter area.
- ✓ Establish productive ground rules if unreasonable behavior persists.
- ✓ Calmly describe the consequences of any discourteous/disruptive behavior.
- ✓ Break big problems into smaller, more manageable problems.
- ✓ Accept criticism in a positive way.
- ✓ When a complaint may be true, use statements such as "You're probably right" or "It was my fault."
- ✓ If the criticism seems unwarranted, ask clarifying questions.
- ✓ Ask for the person's recommendations. Repeat back to him/her what you feel he/she is requesting of you.

**DON'T:**

- × Use styles of communications that generate hostility such as apathy, brush-off, coldness, condescension, robotism, going strictly by the rules, or giving the "run-around".
- × Reject all the person's demands from the start.
- × Posture in a challenging stance, such as standing directly opposite someone, hands on hips, or crossing your arms.
- × Make sudden movements that may be threatening. Notice the tone, volume, and rate of your speech.
- × Challenge, threaten, or dare the person.
- × Belittle the person or make them feel foolish.
- × Criticize or act impatiently towards the agitated individual.
- × Make the situation seem less serious than it is.
- × Attempt to bargain with a threatening individual or make false statements or promises that you cannot keep.
- × Try to convey a lot of technical or complicated information when emotions are high.
- × Take sides or agree with distortions.
- × Invade the individual's personal space
- × Make physical contact, point fingers, roll your eyes, staring or use other forms of aggression.
- × Gossip, spread rumors, sabotage.
- × Withhold information that impacts job performance.